

TARTU ÜLIKOOL

Sotsiaalteaduste valdkond

Ühiskonnateaduste instituut

Infokorralduse õppekava

Monika Liister

Privaatsust puudutavad praktilised väljakutsed infotöötaja töös

Lõputöö

Juhendaja: Maris Männiste, MA

Tartu 2018

SISUKORD

| | |
|---|----|
| SISSEJUHATUS | 3 |
| 1. TEOREETILISED LÄHTEKOHAD | 5 |
| 1.1. Privaatsuse ja isikliku informatsiooni määratlemine | 5 |
| 1.2. Infotöötaja mõiste ja kompetentside määratlemine | 7 |
| 1.3. Isikuandmete kaitse põhimõtted | 8 |
| 1.4. Andmete turvalise töötlemise meetmed..... | 11 |
| 1.5. Privaatsust ja isiklikku informatsiooni käsitlevad varasemad uuringud..... | 13 |
| 2. MEETOD JA VALIM..... | 16 |
| 2.1. Uurimismeetod..... | 16 |
| 2.2. Valim | 17 |
| 3. TULEMUSED..... | 20 |
| 3.1 Privaatsus ja selle kaitsega seonduvad probleemid | 20 |
| 3.2. Isikuandmete kaitseks rakendatavad praktikad..... | 24 |
| 3.3. Andmekaitsereformiga kaasnevad muudatused..... | 26 |
| 4. DISKUSSIOON JA JÄRELDUSED | 31 |
| KOKKUVÕTE | 34 |
| SUMMARY | 36 |
| KASUTATUD KIRJANDUS | 38 |
| LISAD | 42 |
| Lisa 1. Intervjuu kava | 42 |

SISSEJUHATUS

Õigus privaatsusele on üks olulisemaid põhiõigusi, mis puudutab iga inimest. Nii kaua kui seda hüve ei riivata, inimesed oma privaatsusõigusele enamasti ei mõtle. Teema muutub aktuaalseks reeglina siis, kui seda õigushüve ohustatakse. Mida rohkem andmeid ringleb, seda suurema tõenäosusega riivatakse mingil hetkel andmesubjektide õigusi.

Informatsioon on saanud infoühiskonnas väga oluliseks käibeobjektiks ning hüveks (Tikk, Nõmper, 2007: 13). Selle saamiseks, säilitamiseks, vahetamiseks luuakse ja arendatakse uusi tehnoloogiaid ning võimalusi. Andmeid, sealhulgas isikuandmeid võib pidada tänapäeval valuutaks, kuna need võimaldavad ettevõtetel jõuda klientideni, saada isikute ja nende eelistuste kohta rohkem teada ning seeläbi müüa oma teenuseid ja tooteid, teenides suuremat majanduslikku tulu. Interneti laialdase leviku tulemusena on aga privaatsusest ja andmekaitsest saanud väga aktuaalne teema, mis ei ole ainult siseriiklik küsimus, vaid üks Euroopa Liidu olulisemaid valdkondi. Tehnoloogia kiire areng ja ülemaailmastumine on ühiskonda põhjalikult muutnud ning tekitanud andmekaitse valdkonnas uusi probleeme ja suurendanud informatsiooniga manipuleerimise võimalusi (Euroopa Komisjon, 2010), millede lahendamiseks tuleb järjepidevalt tegeleda.

Infohaldust saab vaadelda kui distsipliini, mis on tugevalt seotud väga erinevate teiste distsipliinidega. Seega nii muutuv õigusruum, kui ka teatavad piirangud avaldavad üha enam mõju ka infotöötaja igapäeva tööle (Cervone, 2015). Varasemalt ei ole Eestis privaatsuse teemat infotöötaja töö aspektist põhjalikult uuritud. Oma seminaritöös (Liister, 2018) tegelesin privaatsust puudutavate praktiliste väljakutsetega infotöötaja töös avaliku sektori näitel. Saadud tulemustest lähtuvalt uurisin edasiarendusena käesolevas lõputöös infotöötajaid nii avalikus kui erasektoris ja selgitasin välja, millised on nimetatud eriala esindajate jaoks privaatsusust puudutavad konkreetsed probleemid, väljakutsed ja ka teadlikkus.

Privaatsuse temaatika kaardistamine ja kitsaskohtade välja selgitamine infotöötaja vaatenurgast on oluline nii avaliku kui erasektori jaoks ning kui minna üldisemaks, siis on see oluline

põhiseaduslike õiguste teostamise seisukohalt. Usun, et lisaks infotöötajatele võib käesolev uuring pakkuda huvi organisatsioonide juhtkondadele ja pädevale järelvalveasutusele, andes ülevaate võimalikest kitsaskohtadest ning oleks abiks valdkonna korrastamisel. Töö kaardistab hetkeolukorra ja on baasiks järgmiste uurimistööde tegemisel või ka näiteks Andmekaitse Inspeksioonile täiendavate juhiste välja töötamiseks.

Eesmärgi saavutamiseks püstitasin järgnevad uurimisküsimused, millele otsin vastust semistruktureeritud intervjuude kaudu:

1. Millised on privaatsust puudutavad sagedasemad probleemid infotöötaja töös?
2. Milliseid praktikaid rakendatakse isikuandmete kaitseks?
3. Millised on olulisemad andmekaitsereformiga kaasnevad muudatused organisatsioonide töös?

Lõputöö jaguneb neljaks peatükiks. Esimeses peatükis annan ülevaate töös kasutatud mõistetest, isikuandmete kaitse põhimõtetest, andmete turvalise töötlemise meetmetest ning varasematest uuringutest. Teine peatükk keskendub lõputöö raames läbiviidud uuringule ning esitan valimi ja uurimismetoodika kirjelduse. Kolmandas peatükis esitlen kvalitatiivse uurimismeetodi käigus kogutud tulemusi, neljandas analüüsin tulemusi lähtudes uurimisküsimustest ja teen ülevaate järeldustest.

Täna oma juhendajat meeldiva koostöö, panustatud aja ja asjalike suuniste ning intervjuueeritavaid konstruktiivsete vastuste ja mõtteavalduste eest.

Käesolevat lõputööd iseloomustavad järgmised märksõnad: infotöötaja, andmekaitsereform, privaatsus, isiklik informatsioon, andmete töötlemine.

1. TEOREETILISED LÄHTEKOHAD

Järgnevalt annan ülevaate privaatsuse sisu erinevatest käsitlustest ning rahvusvaheliste ja siseriiklike õigusaktide vastavatest sätetest. Defineerin infotöötaja mõiste, määratlen tema kompetentsid ja kokkupuutepunktid privaatsuse temaatikaga, isikuandmete kaitse põhimõtted ning andmete turvalise töötlemise meetmed. Peatükk annab samuti ülevaate valdkonna varasemate uuringute tulemustest.

1.1. Privaatsuse ja isikliku informatsiooni määratlemine

Privaatsuse olulisus on kerkinud üha rohkem päevakorda viimastel aastakümnetel. Seda on põhjustanud ühiskonda iseloomustavate andmete, sealhulgas inimeste isikliku informatsiooni suurenev kogumine, mis on omakorda seotud tehnoloogiate, võrgustike ning säilitusvahendite arengu ja laialdase kättesaadavusega (Sweeney, 2002: 557). Nimetatud arengute valguses pööratakse üha rohkem tähelepanu just informatsiooni sisule, et kaitsta ning säilitada privaatsust. Informatsioon annab selle valdajale võimu, mistõttu on eriti oluline kaitsta just üksikisiku õigusi andmete töötlemisel tekkida võivate võimalike kuritarvitamiste eest.

Õigust privaatsusele on hinnatud juba palju varem, kui see leidis tunnustamist ja kaitsmist õigushüvena (Männiko, 2011). Põhjalikuma privaatsuse sisu uurimisega on tegeletud alates 20. sajandi teisest poolest. Uurijad on seostanud privaatsust nii sotsiaalsete suhete loomise kui säilitamisega (Fried, 1968: 477), samuti on leitud, et privaatsuse tunnuseks saab pidada autonoomsust (Westin, 1970, Altman 1976: 9 kaudu). Lisaks seostatakse seda isikliku informatsiooni ja selle kontrollimisega (Shils, 1966: 282), kuid infoajastul käsitletakse privaatsust eelkõige kui teiste inimeste ligipääsu takistamist erinevatele isiklikele kommunikatsioonivahenditele ja indiviidi tegevustele internetis (Finn, Wright, Friedewald, 2013).

Männiko (2011) määratleb privaatsust isiku eraelulise sfäärina, milles on isikul õigus otsustada, kas ja kui palju ta oma eraelu teiste inimeste, avalikkuse ja riigiga jagab. Privaatsust on defineeritud samas ka ruumilise ja intellektuaalse sfäärina, mis võimaldab inimesel otsustada teda

puudutavate asjaolude üle, kontrollida, kellel on ligipääs teda puudutavale informatsioonile, luua ja arendada erinevaid suhteid (Palm, 2009). Lähtuvalt eeltoodust saab privaatsust käsitleda kui igaühe õigust enesemääratlemisele, õigust elada minimaalse välise sekkumisega oma soovide ja tahtmiste kohaselt (Maruste, 2004). See annab justkui võimaluse kontrollida inimest iseloomustavat informatsiooni, mis teeb võimalikuks luua terviklik pilt tema olemusest läbi väärtushinnangute, sotsiaalsete suhete ja ka füüsiliste ning virtuaalsete toimingute.

Õigust privaatsusele sätestavad ühe põhiõigusena nii rahvusvahelised õigusaktid kui ka riikide konstitutsioonid. Euroopa kontekstist on andmekaitse ja privaatsusõiguse üks olulisemaid alustalasid inimõiguste ja põhivabaduste kaitse konventsiooni (Inimõiguste..., 2010) artikkel 8. Nimetatud artikkel sätestab igaühe õiguse sellele, et austataks tema era- ja perekonnaelu ning kodu ja sõnumite saladust (Inimõiguste..., 2010). Ametivõimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks (Inimõiguste..., 2010).

Õigus privaatsusele on sätestatud ka ÜRO inimõiguste ülddeklaratsiooni (2013) artiklis 12, mille kohaselt ei või kellegi era- ja perekonnaellu meelevaldselt sekkuda, kellegi kodupuutumast, kirjavahetuse saladust või au ja head nime ei tohi meelevaldselt määrada. Igaühel on õigus seaduse kaitsele taolise sekkumise ja teotamise korral. Samuti kajastab privaatsust puudutavat ka Euroopa Liidu põhiõiguste harta (2007) artikkel 7, mille kohaselt on igaühel õigus sellele, et austatakse tema era- ja perekonnaelu, kodu ja edastavate sõnumite saladust.

Isikuandmete töötlemine on väga tihedalt seotud õigusega privaatsusele. Eesti Vabariigi põhiseadus (2015) ei sätesta eraldi isikuandmete kaitset, küll aga on see tuletatav põhiõiguste kaudu. Täpsed reeglid ning töötlemise põhimõtted, millest juhinduda olid uurimistöö käigus intervjuude läbiviimise ajal sätestatud isikuandmete kaitse seaduses (2016) ja alates 25.05.2018 kohaldatavas EL isikuandmete kaitse üldmääruses (2016).

Andmete põhiõigustega kaitsmine ei keela nende töötlemist, kuid paneb riigile kohustuse reguleerida töötlemist ning kaaluda selle vajalikkust (Pilving, 2005). Seega on väga oluline määratleda privaatne informatsioon ja tagada selle igakülgne kaitse.

1.2. Infotöötaja mõiste ja kompetentside määratlemine

Steineroval (2001) käsitleb infotöötajaid kui inimesi, kes haldavad ja korraldavad erinevates infoasutustes inforessursse ning valdkonna professionaalidena aitavad määratleda kasutajate infovajadusi, juhatahes nad seejärel infoallikateni. Infotöötajate ülesanne on pakkuda kasutajale teavet, infotooteid ja -teenuseid erineva teabe otsingul (Steineroval, 2001). Üldistavalt saab infotöötajat määratleda kui vastava koolitusega spetsialisti, kes tegeleb infoteenindusega ning omab nii tehnilisi kui organisatoorseid teadmisi, oskusi, mis on vajalikud teabe leidmiseks ja edastamiseks.

Käesolevas uurimuses kitsendasin selle definitsiooni tähendust ja fookusseerisin dokumendihalduse suunale, koondades mõiste „infotöötaja“ alla nii avaliku kui erasektori teenistujad, kelle ametikohustuste hulka kuulub asutuse asjaajamise ja dokumendihalduse korraldamine. Näiteks võib selliseks töötajaks asutuses olla kantselei juhataja, dokumendihaldur, referent, sekretär, büroojuht jne. Tegemist on seega spetsialistidega, kelle tähta on oluline roll organisatsiooni kommunikatsiooniprotsessis.

Dokumendihalduri kutsestandard tase 6 (2014), mis kehtib kuni 04.12.2019, kirjeldab nimetatud spetsialisti tööülesandeid järgmiselt: luua ja hoida organisatsioonis kasutusel toimiv info- ja dokumendihaldus; luua, edastada, võtta vastu ja saata välja dokumente, organiseerida dokumendisüsteemi; jälgida info- ja dokumendihalduse toimimist; korraldada dokumentidele juurdepääs ning tagada nende alalhoid ja säilitamine. Dokumendihalduri töö on integreeritud üldisesse organisatsiooni infohaldusesse ja tema tööülesanded võivad osaliselt kattuda teiste info- ja tegevate kutsealade töötajate ülesannetega (Dokumendihalduri..., 2014). Nagu kutsestandardist nähtub, on infotöötaja ametitegevus seotud tihedalt erinevate valdkondadega ning nii muutuv õigusruum kui ka teatavad piirangud avaldavad seeläbi mõju tema igapäevastele töökohustustele (Cervone, 2015) ja nõutavale kompetentsile.

Viimase 20 aasta jooksul on informatsiooni haldamises toimunud paradigma muutus, mis on mõjutanud infotöötaja rolli ja ülesandeid nii era- kui avalikus sektoris (Lomas, 2010). Selle ajendiks on paberdokumentide füüsilisest haldamisest üleminek dokumendi kontrollitud haldamisele infosüsteemis. Dokumendihaldus on liikunud maailmast, kus on suudetud kontrollida ja hoida informatsiooni, sealhulgas isikuandmeid, organisatsiooni piires; maailma, kus asutuse dokumente luuakse ja menetletakse Web 2.0 või pilvetechnoloogia abil kaugel organisatsiooni piiridest väljas (Lomas, 2010). Ulatuslikud muutused ühiskonnas, infomajanduse globaalne

iseloorm, samuti muutunud töökeskkond nõuavad infotöötajatelt uusi ja keerukamaid pädevusi rohkem kui varem (Myburgh, 2003). Kaasaegne infotöötaja peab toime tulema uute järjest kasvavate elektrooniliste inforessurssidega. Dokumendihalduri kutsestandard tase 6 (2014) sätestab, et dokumendihaldur teeb infotehnoloogiliste süsteemide toimimise tagamisel koostööd infotehnoloogia spetsialistiga, sest info- ja dokumendihalduse süsteem on nii sisuline kui tehnoloogiline.

Infoühiskonnaga kaasnenud uutele võimalustele lisaks tuleb infotöötajal arvestada ka kaasnevate ohtudega, sealhulgas andmete turvalisusega. Näiteks pilveteenuste puhul on kontroll turvalisuse üle olulises osas teenuseosutaja käes ja seetõttu peab kasutaja saama hinnata, kas teenuseosutaja on täitnud turvanõudeid käideldavuse, terviklikkuse ja konfidentsiaalsuse osas (Pilvandmetöötlus, 2014). Isikuandmete sisestamisel süsteemi ei pruugi pilveteenuse kasutaja olla enam ainus, kes neid andmeid kontrollib. Ebapiisav teave pilveteenuse töötlemistoimingute kohta tähendab riski nii pilveteenuse kasutajale kui ka andmesubjektide jaoks (Pilvandmetöötlus, 2014) ja sellega tuleb arvestada. Töötlemine saab alguse andmete kogumise momendist, seega peab juba algfaasis rakendama isikuandmete kaitseks kõiki vajalikke meetmeid.

Lisaks erialastele teadmistele ja õigusaktide tundmisele seab töö isikuandmetega ning muu konfidentsiaalse informatsiooniga dokumendihaldurile kõrged eetilised nõudmised (Dokumendihalduri..., 2014), mille tähendust ei saa samuti alahinnata.

Kokkuvõttes saab öelda, et organisatsioonilised muutused, tehnoloogia kiire areng, globaliseerumine, digitaalressursside kiire kasv nõuavad uusi pädevusi ning tänapäeval on infotöötaja spetsialist, kes lisaks erialastele teadmistele peab orienteeruma nii infotehnoloogia, õiguse, kommunikatsiooni kui kvaliteedijuhtimise valdkondades. Suutma pidevalt täiustada ja edasi arendada omandatud teadmisi ning oskusi.

1.3. Isikuandmete kaitse põhimõtted

Dokumendihaldur puutub oma igapäevatoos kokku konfidentsiaalse informatsiooniga, sealhulgas töö isikuandmetega, sageli korraldades sellele juurdepääsu (Dokumendihalduri kutsestandard, 2014). Kaasaegse isikuandmete kaitse sisuliseks lähtekohaks on eelkõige isiku õigus privaatsusele ehk eraelu kaitse. Isiku eraelu kaitse on küll peamine väärtus, mida nimetatud valdkonna regulatsioonid tagavad, kuid andmekaitse õigusakte ajakohastatakse eesmärgiga tagada ka muid

privaatsusega seotud huvisid nagu näiteks infosüsteemide turvalisus, neis sisalduvate andmete kvaliteet, läbipaistvus, individuaalse osaluse põhimõte.

14.04.2016 kiitis Euroopa Parlament heaks isikuandmete kaitse üldmääruse (2016), millega asendati senine andmekaitse direktiiv. Tegemist on otsekohalduva määrusega, mis koos siseriiklike rakendusaktidega asendab varasemalt Eestis kehtinud isikuandmete kaitse seadust (2016). Määrus jõustus 24.05.2016 ja seda kohaldatakse alates 25.05.2018 (Euroopa andmekaitse reform, 2017). Nimetatud muudatus õigusaktides ei toonud kaasa aga andmekaitseõiguse vundamendi kardinaalset muutmist, vaid jätkuvad edasi enne üldmääruse kohaldamist kehtinud ja Eesti seadusandluses sätestatud põhimõtted.

Tulenevalt asjaolust, et viisin uuringu läbi ajal, mil kehtis isikuandmete kaitse seadus (2016), toon alljärgnevalt teooria peatükis välja nii uuringu ajal kehtivad regulatsioonid, kui üldmääruse (EL..., 2016) eesmärgid ning olulisemad muudatused, millega pidid organisatsioonid peale 25.05.2018 arvestama ja mille täitmiseks ettevalmistusi tegema.

Isikuandmete kaitse seaduse (2016) paragrahv 4 defineerib isikuandmed järgmiselt: isikuandmed on mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. Üldmäärus (EL..., 2016) esitab vastava definitsiooni artiklis 4. Delikaatseteks isikuandmeteks loetakse vastavalt isikuandmete kaitse seadusele (2016) poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmeid, välja arvatud andmeid seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta; etnilist päritolu ja rassilist kuuluvust kirjeldavad andmeid; andmeid tervises seisundi, puude, pärilikkuse informatsiooni kohta; biomeetrilisi andmeid; andmeid seksuaalelu, ametiühingu liikmelisuse, süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist. Üldmäärus (EL..., 2016) ei kasuta enam mõistet „delikaatsed isikuandmed“, vaid seda asendab mõiste „eriliiki isikuandmed“, kuid mõiste sisu on jäänud samaks. Artikkel 51 (EL ..., 2016), sätestab, et sellist laadi isikuandmed, mis on oma olemuselt põhiõiguste ja -vabaduste seisukohast eriti tundlikud, väärivad erilist kaitset, sest nende töötlemise kontekst võib põhiõigusi ja -vabadusi olulisel määral ohustada.

Isikuandmete kaitse seaduse (2016) kohaselt on isikuandmete töötlemine iga isikuandmetega tehtav toiming sõltumata selle teostamise viisist ja kasutatavatest vahenditest. Näiteks nende kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine, päringute teostamine ja väljavõtete tegemine, kasutamine, edastamine,

riskikasutamine, ühendamine, sulgemine, kustutamine, hävitamine, või mitu eelnimetatud toimingut. Töötlemise definitsioon on jäänud oma olemuselt samaks ka üldmääruses (2016). Kuigi suur osa andmetöötlustest infotehnoloogia ajastul toimub automatiseeritult, on oluline kaitsta ka käsitsi või paberkandjal toimivas andmetöötlustes kasutatavat teavet. Isikuandmete töötlemise mõiste hõlmab endas nii käsitsi kui automatiseeritult tehtavat andmetöötlust.

Isikuandmete kaitse seadus (2016) määratles põhimõtted, mida töötleja oli kohustatud järgima alljärgnevalt: seaduslikkuse põhimõte, eesmärgikohasuse põhimõte, minimaalsuse põhimõte, kasutuse piiramise põhimõte, andmete kvaliteedi põhimõte, turvalisuse põhimõte, individuaalse osaluse põhimõte. Üldmäärus (EL..., 2016) sätestab isikuandmete töötlemise põhimõtted artiklis 5 ning need ei erine eeltoodust.

Alates 25.05.2018 kohaldatava isikuandmete kaitse üldmääruse peamiseks eesmärgiks on vajadus suurendada läbipaistvust ja kontrolli isikuandmete üle (Euroopa Komisjon, 2010). Võimalus kontrollida eeldab endast aga läbipaistvust isikuandmete töötlemisel, samuti peab isikutele esitatav teave nende andmete töötlemise kohta olema arusaadav (Euroopa Komisjon, 2014). Seejuures tuleb kasutada selget ja lihtsat keelt ning töötleja kehtestatud isikuandmete töötlemise ja andmesubjektide õiguste kaitsmise põhimõtted tuleb teha lihtsalt kättesaadavaks. Üldmäärus (EL..., 2016) näeb ette õiguse tutvuda enda kohta kogutavate andmetega.

Lisaks eeltoodule on regulatsiooni eesmärgiks lahendada ebaselgus isikuandmete töötlejate vastutuse osas. Näiteks pilveandmetöötlustes ei salvestata andmeid füüsilistele andmekandjatele, vaid kogu protsess alates kogumisest toimub pilves. Nimetatud juhul on tavaline, et pilvetöötlustes osaleb mitmeid töötlejaid (pilve haldaja, internetiteenuse pakkuja), mistõttu võib andmesubjektil osutada raskeks tuvastada, kes ning millisel alusel tema andmeid töötleb (Pilvandmetöötlus, 2014). Üldmäärus (EL..., 2016) näeb ette vastutuse printsiibi, mis nõuab vastutavalt töötlejalt meetmete rakendamist tagamaks andmete töötlemise kooskõla määrusega ning samuti peab vastutav töötleja neid meetmeid järelvalveasutusele vajadusel demonstreerima.

Uue mõistena toob üldmäärus (EL..., 2016) sisse „õiguse olla unustatud“. Õigus enda andmete kustutamisele suurendab andmesubjekti kontrolli nende üle ja annab talle võimaluse otsustada, mis saab tema andmetest peale nende avalikustamist. Õiguse andmete kustutamisele sätestab artikkel 17 (EL..., 2016). Muutunud on ka tõestuskoormis – ettevõtte on kohustatud tõendama, miks on vajalik andmesubjekti andmete jätkuv töötlemine. Sisuliselt oli õigus nõuda oma andmete kustutamist sätestatud juba isikuandmete kaitse seaduses (2016). Seda saab nõuda üksnes nende andmete osas, mida töödeldakse nõusoleku alusel või mille töötlemiseks puudub õiguslik alus.

Uueks nõudeks on isikuandmete ülekantavus, mis sisuliselt võimaldab isikul võtta oma digitaalsed andmed ühest ettevõttest ning viia teise ettevõttesse. Vältida soovitakse seega olukorda, kus teenusepakkuja vahetamine tooks kaasa isikule isiklikult ja samuti sotsiaalselt olulise informatsiooni kadumise. Seega on ettevõtetel mõistlik kulude optimeerimiseks ning klientide rahulolu suurendamiseks oma infosüsteemid muuta selliseks, mis võimaldavad andmeid võimalikult hõlpsalt ja lihtsalt üle kanda üldkasutatavas masinloetavas vormingus (Kuidas..., 2017). Andmete ülekantavust tuleb rakendada nii era- kui avalikul sektori asutustel.

Kokkuvõttes saab konstateerida, et kuigi alates 25.05.2018 kohaldatakse üldmääruses (EL..., 2016) sätestatud, ei ole isikuandmete töötlemise põhimõtted muutunud, lisandunud on uusi mõisteid, millega peavad organisatsioonid arvestama ning mis eeldab mõningatel juhtudel näiteks infosüsteemides täiendavate funktsionaalsuste loomist. Kuigi määrus sisaldab era- ja avalik sektori jaoks arvestatavaid erisusi, ei seisne need andmete töötlemises, vaid andmekaitespetsialisti määramises ja tervikhindamise läbiviimise vajalikkuses.

1.4. Andmete turvalise töötlemise meetmed

Isikuandmete kaitse tähtsustumine on tingitud asjaolust, et isiku eraelu ei olnud varasematel aegadel võimalik rünnata nõnda nagu tänapäeval, kui saab luua andmebaase ning isikuandmeid automatiseeritult töödelda (Ilus, 2002: 442). Tehnoloogia areng on kaasa toonud suuremad turvariskid. Tulenevalt üldmääruse (EL..., 2016) artiklist 32 on andmete töötleja (nii vastutav kui ka volitatud) kohustatud rakendama andmetele vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslike meetmeid. Samuti on vastutav ja volitatud töötleja kohustatud võtma tarvitusele meetmed, et volituse alusel tegutsevad isikud, kellel on juurdepääs isikuandmetele, töötlevad neid ainult vastutava töötleja juhiste alusel (EL..., 2016).

Andmetöötluse turvalisust ei saavutata üksnes sobiva tark- ja riistvara kasutusele võtmisega, vaid lisaks sellele peavad olema kasutusele võetud ka organisatsioonilised meetmed ja reeglid nende elluviimiseks. Organisatsiooniliste meetmetena tuuakse juhistes välja näiteks töötajate regulaarset koolitamist ja teavitamist andmeturbe valdkonnast, juurdepääsuõiguste reguleerimist asutuses, konkreetset, selget ülesannete ning pädevuste jaotust isikuandmete töötlemisel aga ka auditite korraldamist organisatsioonis (Handbook..., 2014: 94). Ka isikuandmete kaitse seadus (2016) § 26 paneb töötlejale kohustuse tagada oma alluvuses isikuandmeid töötlevate isikute kohane koolitus. Lisaks kohustab seadus töötajat hoidma saladuses talle tööülesannete täitmisel teatavaks

saanud isikuandmeid ka pärast töötlemisega seotud tööülesannete täitmist või töö- või teenistussuhte lõppemist.

Seega on nii era- kui avaliku sektori asutuste ülesanne ja kohustus teada täpselt, milliseid isikuandmeid ja kuidas töödeldakse, kuidas hoitakse, kellel on nimetatud andmetele juurdepääs ja millised on andmesubjekti õigused ning tagada töötajate andmekaitsealane väljaõpe. Samuti on asutuse töötajatel, kes töötlevad ametiülesannete täitmiseks isikuandmeid, kohustus järgida õigusaktidest tulenevaid ning asutuse poolt kehtestatud regulatsioone, vältimaks andmete väärkasutust. Avaliku teabe valdaja peab lisaks avaliku teabe seaduse (2016) § 43 kohaselt tagama, et juurdepääsupiiranguga teave ei satuks pääsuõigusteta isikute kätte.

Teabe privaatsus on tihedalt seotud infoturbega. Isikuandmete kaitse seadus (2016) § 25 lõige 2 loetleb turvameetmed, mida isikuandmete töötleja on kohustatud järgima:

- 1) vältima kõrvaliste isikute ligipääsu andmetöötlusseadmetele;
- 2) ära hoidma andmete omavolilist lugemist, kopeerimist, kustutamist jms;
- 3) tagantjärele peab olema võimalik kindlaks teha, kes, millal, millele juurde pääses, salvestas; muutis või kustutas ning kellele, millal ja miks isikuandmeid edastati;
- 4) tagama, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs üksnes talle töötlemiseks lubatud andmetele ja töötlemisviisidele – infosüsteemidesse sisenemiseks kasutatakse identifitseerimist ja autentimist, juurdepääsuõiguste haldamine;
- 5) tagama, et isikuandmete edastamisel andmesidevahenditega ja andmekandjate transportimisel ei toimuks isikuandmete omavolilist lugemist, kopeerimist, muutmist või kustutamist – näiteks andmete edastamisel kasutatakse krüpteerimist;
- 6) kujundama ettevõtte, asutuse või ühenduse töökorralduse niisuguseks, et see võimaldaks täita andmekaitse nõudeid – näiteks info- või privaatsuspoliitika väljatöötamine asutuses.

Andmetöötluse turvalisusega seoses kehtestab üldmäärus tervikluse põhimõtte ehk kohustuse töödelda isikuandmeid viisil, mis kaitseb neid loata või ebaseadusliku töötlemise, juhusliku kaotamise, hävitamise või kahjustamise eest kasutades nõuetekohaseid tehnilisi või organisatsioonilisi meetmeid.

Lõimitud andmekaitse on aga põhimõte, mille kohaselt kohustub andmete töötleja arvestades teaduse ja tehnika arengut, parimaid rahvusvahelisi tavasid ning andmetöötlumisest tulenevaid riske, võtma töötlemise eesmärkide ja vahendite valikul ning töötlemise käigus kasutusele selliseid proportsionaalseid tehnilisi ja organisatsioonilisi meetmeid, millega tagatakse töötlemise vastavus EL isikuandmete kaitse üldmääruse (EL..., 2016) nõuetele ning andmesubjekti õiguste kaitse.

Lõimitud andmekaitset saab pidada privaatsust parandavate tehnikate ja tehnoloogiate kasutamiseks andmetöötlustoimingute läbiviimisel nagu e-ID põhised või kaheastmelised autentimislahendused, isikuandmete edastamisel kasutatavad turvalahendused (VPN), isikuandmete krüpteerimine, toimingute korrektne logimine infosüsteemides jne (Vaikimisi..., 2017). Lõimitud kaitsel pööratakse erilist tähelepanu kogu isikuandmete olelusringi haldamisele alates kogumisest, töötlemisest kuni kustutamiseni.

Kolmanda uue põhimõttena on vastutuse põhimõte, mis paneb töötlejale laialdase vastutuse tema korraldatava ja tema nimel toimuva isikuandmete mis tahes töötlemise eest, muuhulgas seoses andmete turvalisuse ja mõjuhinnangutega. Määruses sätestatud reeglite kaudu peaks vastutav töötleja tagama eelkõige iga töötlemistoimingu kooskõla üldmäärusega (EL..., 2016), samuti peaks ta suutma antud kooskõla tõendada.

Kokkuvõttes saab konstateerida, et ühelt poolt on organisatsioonidele (töötlejatele) kehtestatud andmetöötluse regulatsioonid, millede järgmine on kohustuslik, teisalt peab ka infotöötaja isikuandmeid töödeldes järgima kõiki kehtestatud nõudeid, sealhulgas tööandja poolt väljatöötatud juhendeid. Samuti on asutustel kohustus tagada oma alluvuses isikuandmeid töötlevate isikute kohane koolitus ja väljaõpe.

1.5. Privaatsust ja isiklikku informatsiooni käsitlevad varasemad uuringud

Käesolevas alapeatükis annan ülevaate varasematest privaatsust ja isiklikku informatsiooni käsitlevatest uuringutest ning nende eesmärkidest ja tulemustest. Esitatud uuringud aitavad mõista teema olulisust ja aktuaalsust ning on lähtekohaks lõputöö raames läbiviidud uurimusele.

Privaatsuse puhul saab rääkida eelkõige informatsiooni privaatsusest. Varasemate uuringute tulemusi analüüsides saab välja tuua, et privaatsust seostatakse isikliku ja eraelulise informatsiooniga, väärtustatakse inimese õigust ise otsustada, kui palju isiklikku teavet enda kohta avaldada soovitakse, seega väärtustakse nii enda kui teiste inimeste privaatsust (Tihonov, 2015, Liister, 2018). Isikliku informatsiooni alla liigitatakse peamiselt perekonda, tervist ning majanduslikku olukorda kirjeldavad andmed (Tihonov, 2015). Taolise määratluse on välja toonud ka Baek ja kolleegid (2014: 525), Witzner ja kolleegid (2008: 84) ning MacDondald ja Streatfeild (2014: 626). Täpsemalt kirjeldatakse isiklikku informatsiooni kui ressursi, mille kaudu on võimalik inimest identifitseerida (Tihanova, 2015; Liister, 2018). Uuringute (Tihanova, 2015)

tulemustest selgub, et oluliseks peetakse tööandja poolt töötajate isikliku informatsiooni turvalisuse tagamist ning ollakse pigem häiritud, kui asutus kogub liiga palju töötajaid puudutavat informatsiooni.

Samas on varasemad uuringud välja toonud aspekti, et privaatsust võidakse tõlgendada erinevalt. Teatud juhtudel mõjutavad privaatsuse väärtustamist inimese demograafilised näitajad, inimese vanus ja ametipositsioon (Tihanova, 2015). Tihanova (2015) magistritöö tulemused näitasid, et uuringus osalenud mittejuhid (spetsialistid) peavad privaatsuse väärtustamist olulisemaks kui teevad seda näiteks juhid. Teisalt tõstatas minu seminaritöös (Liister, 2015), kus intervjuueeritavateks olid avaliku sektori infotöötajad, üles just juhtide rolli olulisus.

Smith ja tema kolleegide (1996) poolt läbi viidud uuringu tulemused näitasid, et isikuandmete turvalisuse pärast muretsemist võivad mõjutada ka eelnevad negatiivsed kogemused. Inimene, kes on varasemalt kokku puutunud informatsiooni kuritarvitamisega, tunneb tõenäoliselt tõsist muret oma isikliku informatsiooni turvalisuse üle. Uurijad tõid välja asjaolu, et mida olulisemaks peeti informatsiooni turvalisust, seda tõenäolisemalt välditakse tulevikus tegevusi, mis eeldavad isikliku teabe avaldamist (Smith, Smith, Milberg, 1996: 171, 173). Privaatsuse temaatika on inimeste jaoks oluline, mistõttu on tähtis austada ka teiste inimeste soovi privaatsusele (Tihonov, 2015; Liister, 2018). Kui Tihanova uurimuse kohaselt pidasid vastajad oluliseks oma isikliku informatsiooni turvalisust, siis minu (2018) seminaritöö tõi välja asjaolu, et andmekaitse reeglite vastu eksinud teenistujad on küll sageli kriitilised enda kohta käivate delikaatsete isikuandmete lekkimise ohu osas, kuid teiste privaatse informatsiooni ohtu seadmisel ei suudeta tagajärgi näha.

Cooper'i (2016) poolt läbi viidud uuringust nähtus, et infotöötajate praktikaid privaatsuse ja andmekaitse osas mõjutavad nii isiklikud hoiakud, kui isiklikud ning professionaalsed kogemused. Toodi välja, et kuigi asutustes on kehtestatud piisavad protseduurid, ei tutvustata neid vajalikus mahus töötajatele ning töötajate ebapiisav koolitamine on mõjutanud õigusaktidest tulenevate privaatsust ja isikuandmete kaitset puudutavate kohustuste täitmist. Koolitamise olulisus joonistus välja samuti minu seminaritöö (Liister, 2018) käigus läbi viidud uuringu tulemusi analüüsides. Nii infotöötajate endi, kui teiste töötajate ebapiisav koolitamine mõjutab otseselt privaatsust ja isikuandmete kaitsega seonduvate kohustuste täitmist ning andmetöötluse kvaliteeti (Cooper, 2016; Liister, 2018). Lisaks näitasid seminaritöö (Liister, 2015) tulemused, et isikuandmete kaitse valdkonnas on avalikus sektoris sisekoolitaja ülesanded määratud just infotöötajatele.

Infotöötaja rolli Euroopa Liidus läbiviidavas andmekaitse reformis ning uute regulatsioonide kehtestamisega kaasnevaid võimalikke muudatusi uurisin oma seminaritöös (Liister, 2018).

Cornelissen (2008) toob välja, et teenistujad on oma töös pühendunud, kui nad saavad otsustusprotsessides kaasa rääkida ja nende arvamusega arvestatakse. Avaliku sektori näitel läbi viidud uuring näitas aga infotöötajate madalat kaasatust ja puudulikku teadlikkust üldmääruse (EL..., 2016) kohaldamisest ning vähest informeeritust organisatsiooni tegevustest uuendusteks valmistumisel (Liister, 2018). Samas rõhutavad privaatsust puudutavad uuringud (Cooper, 2016; Liister, 2018) just andmetöötajate koolitamise olulisust, tagamaks tõhusam privaatsuse kaitse.

Toetudes varasematele uuringutele, saab väita, et privaatsus ja isikliku informatsiooni temaatika on aktuaalne ning samuti peetakse tähtsaks isikliku informatsiooni turvalisust. Mitmetes välja toodud töödes jõuti järeldusele, et peamiseks viisiks vältida privaatsuse rikkumist ja negatiivsete tagajärgede tekkimist on säilitada kontroll isikliku informatsiooni üle. Samuti on isikuandmete kaitse aspektist oluline infotöötajate ja teiste isikuandmeid töötlevate teenistujate teadlikkuse tõstmine, õigusaktidest tulenevate põhimõtete tundmine, koostöö erinevate valdkondade esindajatega ning juhtkonnaga.

2. MEETOD JA VALIM

Käesolevas peatükis annan ülevaate uuringus kasutatud meetodist ning kirjeldan valimi moodustamist.

Uurimistöö eesmärk on kaardistada privaatsust puudutavad praktilised väljakutsed infotöötaja töös era- ja avalikus sektoris ning lähtudes püstitatud eesmärgist otsin vastuseid järgmistele uurimisküsimustele:

1. Millised on privaatsust puudutavad sagedasemad probleemid infotöötaja töös?
2. Milliseid praktikaid rakendatakse isikuandmete kaitseks?
3. Millised on olulisemad andmekaitsereformiga kaasnevad muudatused organisatsioonide töös?

2.1. Uurimismeetod

Lõputöös kasutasin andmete kogumiseks kvalitatiivse uurimismeetodina semistruktureeritud intervjuud, mille paindlikus võimaldab selle läbiviijal saadud vastuste sisust tulenevalt varieerida käsitletavate teemade järjekorda ning esitada täiendavaid küsimusi (Hirsjärvi, Remes ja Sajavaara, 2010) ning seeläbi saada kätte võimalikult palju olulist informatsiooni.

Uurimisküsimustele vastuste leidmiseks intervjuueerisin nelja erasektori ja nelja avaliku sektori infotöötajat ning intervjuude käigus saadud andmete analüüsimisel keskendusin tähendustele ja tõlgendustele, mida uuringus osalejad väljendasid (Laherand, 2008). Andmete kogumiseks vajalike intervjuude läbi viimiseks koostasın uurimisküsimustest lähtuvalt intervjuu kava (Lisa 1), mis sisaldas kolme alateemat.

Esimese alateema moodustavad privaatsust puudutavad küsimused, mis avavad eeltoodud mõiste sisu ning tähenduse infotöötaja jaoks, toovad välja tööülesanded, mille käigus infotöötaja puutub kokku privaatsuse informatsiooni töötlemisega ja samuti isikuandmete töötlemisega seonduvad probleemid. Teises alateemas on isikuandmete kaitsega seonduvad küsimused, mille koostamisel

soovisin saada informatsiooni asutuses kasutusel olevatest praktikatest ning isikuandmete kaitseks rakendatavatest meetmetest. Kolmandas alateemas on küsimused, mis puudutavad andmekaitsereformi, organisatsioonis plaanitavaid muudatusi, infotöötaja rolli neis ja kaasnevaid võimalikke uuendusi infotöötaja igapäevatoos. Intervjuu kava küsimustiku koostamisel tuginesin lõputöö esimeses peatükis esitatud teoreetilisele osale ning õigusaktides sätestatule.

Intervjueeritavatega kontakteerusin kohtumise kokku leppimiseks telefoni teel. Uuringus osalemine oli vabatahtlik ning selgitasin osalejatele lõputöö eesmärki. Intervjuud viisin läbi ettevalmistatud kava alusel vabade vastustega intervjuu vormis.

Küsimuste täpset sõnastust ja nende järjekorda võisin varieerida vastavalt uuringus osalejate poolt antud vastuste sisule, intervjuu käigule ning vajadusel esitasin täiendavaid küsimusi. Intervjuud viisin läbi suuliselt, vahetu vestluse käigus. Kohtumise aja ja koha said infotöötajad valida ise. Keskmine vestluse kestus oli 40 minutit. Intervjuud lindistasin ja dokumenteerisin transkribeerimise teel.

Transkriptsioonides ja uuringu analüüsis on intervjueeritavad märgitud vastavalt vestlemise järjekorrale A1, A2, A3, A4, E1, E2, E3 ja E4. Intervjueerimisel saadud andmeid kasutasin käesoleva lõputöö eesmärgi saavutamiseks. Selgitasin vastajatele, mis eesmärgil intervjuu tehakse ning seda, et tagan nende isikuandmete, töökohtade ning intervjuu käigus nimetatud kolmandate isikute andmete anonüümsuse ja konfidentsiaalsuse.

Saadud andmete analüüsiks kasutasin kvalitatiivset sisuanalüüsi ja teemapõhist kodeerimist, mille puhul koondatakse sarnase tähendusega tekstiosad, mis sisaldavad nii selgelt välja öeldud kui ka mõista antud sõnumeid vastavate kategooriate alla (Laherand, 2008: 290). Esmalt lugesin transkriptsioonid korduvalt läbi, et kaardistada vastuste tervikut. Teistkordsel intervjuude lugemisel otsisin lähtuvalt lõputöö eesmärgist ja püstitatud uurimisküsimustest tähtsamad mõtted ja märksõnad, tekitades koodide nimetused, mis seejärel ühendasin omakorda kategooriateks. Kodeerimisel kasutasin avatud kodeerimist (Laherand, 2008: 286). Iga kategooria ja koodi iseloomustamiseks leidsin uuringus läbiviidud intervjuudest näiteid.

2.2. Valim

Uurimistöö valimi moodustasin nii avaliku kui erasektori infotöötajatest ning seega pidid intervjueeritavad vastama järgmistele nõuetele: nende tööülesandeks on info- ja

dokumendihalduse korraldamine (infotöötaja) ning nad töötavad kas avaliku või erasektori asutuses. Samuti pidasin valimi moodustamisel silmas, et pooled valimisse kuuluvad isikud oleksid avaliku ja pooled erasektori töötajad. Jälgisin, et intervjueeritavate hulgas oleks esindatud erinevad regioonid üle Eesti. Avaliku sektori puhul oli valimis esindatud ministeeriumi, selle valitsemisala asutuse ja kohaliku omavalitsuse infotöötajad. Erasektorist kuulusid valimisse Eesti ettevõtete ja rahvusvaheliste kontsernide infotöötajad. Valimi moodustamisel ei pidanud ma oluliseks asutuse suurust, kuna uurimuse eesmärgist tulenevalt on fookuses infotöötajate praktilised väljakutsed ja asutuste poolt rakendatavad praktikad, sõltumata organisatsiooni töötajate arvust.

Lõputöö valimi koostamisel oli oluline kaasata nii era- kui avaliku sektori infotöötajad põhjusel, et isikuandmete töötlemist ja kaitset puudutavad regulatsioonid kehtivad kõikidele organisatsioonidele. Erasektori osas ei ole varasemalt analoogseid uuringuid läbi viidud ning kaardistatud infotöötaja väljakutseid nimetatud valdkonnas. Oma seminaritöö (Liister, 2018) edasiarendusena uurin antud lõputöös lisaks avalikule sektorile ka erasektori infotöötaja kokkupuudet isikuandmete temaatikaga, andmetöötlusel tekkinud probleeme, asutuses kasutusel olevaid praktikaid ning organisatsioonides läbiviidud muudatusi vastamaks üldmääruse (EL..., 2016) nõuetele. Kõrvutan kahe sektori erinevusi ning otsin ühisjooni infotöötajate töö aspektist andmekaitse valdkonnas.

Lähtudes eelnevalt toodud valimi moodustamise põhimõtetest saatsin e-kirja juhuslikult valitud viiele avaliku sektori ning 21 erasektori asutusele ja palusin nõusolekut uuringu läbiviimiseks, samuti palusin vastutava infotöötaja kontaktandmeid. Avalikus sektoris keeldus üks asutus põhjusel, et nende infotöötaja on puhkusel ja asendaja ei soovinud uuringus osaleda. Erasektoris jättis kirjale vastamata üheksa asutust, osalemisest keeldus kaheksa. Mitteosalemise põhjusena toodi ühel juhul asjaolu, et tegemist on väikese firmaga, kus andmekaitse pole aktuaalne, kahel juhul toodi põhjusena asjaolu, et pole tutvunud uute regulatsioonidega ning ei soovita asutuse tänast olukorda avaldada, ühel juhul toodi keeldumise alusena kartust uues üldmääruses kehtestatud trahvide ees. Ühel juhul oli asutuse juht nõus, kuid keeldus infotöötaja, kes ei soovinud antud teemal vastata. Kolmel juhul toodi põhjusena vajadust kaitsta ärisaladust ning samuti ei peetud piisavaks garantiiks konfidentsiaalsuslepingu sõlmimist.

Lõputöö jaoks andmete kogumiseks viisin ajavahemikus 02.-07.04.2018 läbi semistruktureeritud intervjuu kaheksa infotöötajaga. Minul, kui lõputöö autoril, puuduvad isiklikud suhted intervjueeritavatega. Tegemist on valimiga, mille tunnused on teatud osades homogeensed

(sarnased) ja teatud osades heterogeensed (omavahel eristuvad). Valimi olulisemaks homogeenseks tunnuseks on see, et intervjueeritavad täidavad infotöötaja töökohustusi, see tähendab vastutavad asutuse asjaajamise- ja dokumendihalduse eest. Heterogeenseteks tunnusteks oli intervjueeritavate vanus ja haridus. Kontrastse valimi põhimõtet toetas ka töötajate erinev kogemus ja ametiaeg ning täidetavad tööülesanded. Kui avalikus sektori intervjueeritavad vastutasid vastavalt tööjuhendis toodule üksnes asutuse asjaajamise ja dokumendihalduse eest, siis erasektoris oli ühe intervjueeritava tööülesanneteks lisaks raamatupidamine ja teisel juhul personalitöö.

Kokkuvõttes saab välja tuua, et erasektori puhul oli valimi kokku saamine raskem, kui avaliku sektori puhul. Üheks teguriks on kahtlemata muudatused andmekaitstes, sellest tulenev teadmatus, mittekursisolek üldmääruse (EL..., 2016) sätetega, hirm trahvide ees ja teisalt soov kaitsta ettevõtte andmeid ning ärisaladust.

3. TULEMUSED

Uuringu käigus läbiviidud intervjuudest selgusid erinevad privaatsust puudutavad väljakutsed infotöötaja töös, mis on käesolevas peatükis käsitletud järgmiste alateemadena:

- Privaatsus ja selle kaitsega seonduvad probleemid;
- Isikuandmete kaitseks rakendatavad praktikad;
- Andmekaitsereformiga kaasnevad muudatused.

3.1 Privaatsus ja selle kaitsega seonduvad probleemid

Uuringu seisukohalt oli oluline välja selgitada, kuidas defineerivad infotöötajad privaatsust. Nii avaliku kui erasektori vastajad seostasid seda isikliku ja eraelulise informatsiooniga. Leiti, et privaatsus on seotud sellega, kui palju isiklikku informatsiooni enda kohta avaldatakse, samuti seostati privaatsust isikliku informatsiooni varjamisega.

E1: Privaatsus kuulub minu jaoks inimese põhiõiguste hulka. See on isiku, või miks mitte ka grupi võimalus hoida teatud asju ainult enda teada, mitte jagada neid teistega, õigus intiimsusele, õigus kontrollida enda kohta saadaolevat infot. Minu eraeluline info on privaatne.

Privaatsete andmetena käsitleti isikuandmeid, täpsemalt andmeid perekonna ja laste kohta, eraelulisi andmeid, põlvnemist, terviseandmeid, finantsandmeid, kontaktandmeid. Avalikus sektoris toodi välja eraldi kategooriana sotsiaalvaldkonna andmed ning erasektoris täpsustati liigina klientide andmed. Avaliku sektori vastajad rõhutasid teenistujate kontaktandmete ja terviseandmete kaitse olulisust, kuna nende andmete kaudu on isik haavatav, samuti käsitleti privaatsetena töölepingu tingimusi.

A2: Eraelulised on minu isikut, perekonda, elukohta, varalist seisut jms puudutavad andmed, ka delikaatsed andmed nagu tervis, põlvnemine, veendumused ja muu. Kindlasti

aga on sellisteks andmeteks veel töötingimusi ja kokkuleppeid, töölepingut puudutavad andmed.

Uuringu tulemused näitasid, et infotöötaja töö on olulisel määral seotud privaatsuse kaitsega ja seda olenemata sektorist. Nimetatud valdkonna esindajad puutuvad ametialaselt kokku suure hulga andmetega, sealhulgas isikuandmetega. Kui avaliku sektori infotöötajad puutuvad privaatsuse kaitsega kokku asutusesisest dokumendiringlust korraldades, siis erasektoris on kokkupuude eelkõige kliendisuhtlusest ja lepingute täitmisest tulenevalt. Tööülesanded, mille raames isikuandmete töötlemine toimub, on avalikus sektoris haldusaktide koostamine, perekonnaseisutoimingute registreerimine, järelevalve tegevus dokumendihaldussüsteemis, dokumentide menetlemine (registreerimine, suunamine menetlusse) nii asutuse üldmeilis kui dokumendihaldussüsteemis, erinevates registrites kannete tegemine ning arhiveerimine. Erasektoris toodi tööülesannetena välja kliendi- ja ärisuhtlus, sealhulgas vastuvõtule registreerimine, konsultatsioon, ankeedid, aruandlus, kirjavahetus ja muu lepingute täitmisega seonduv andmetöötlus. Erinevuseks sektorite osas oli ka asjaolu, et eraettevõtetes lisandus infotöötaja ülesannetele täiendavalt asutuse personalitöö või raamatupidamise korraldamine, samal ajal kui riigiasutustes tegelesid vastajad ainult organisatsiooni asjaajamise ja dokumendihalduse korraldamisega.

E3: Kõik mu tööülesanded on seotud isikuandmetega, näiteks vormistan lepinguid, üldiselt siis ärisuhtlus klientidega – nõustan neid, kogun nende andmeid, näen klientide koduseid aadresse, dokumendi andmeid, telefoni numbreid, kes milliseid makse maksab ja kes kellele rahaülekandeid teeb, mida tellib. Siis tegelen ka nende andmete arhiveerimiseks korrastamisega.

Kui avalik sektor töötleb isikuandmeid seadusest ja põhimäärusest tulenevate eesmärkide saavutamiseks ning lepingute täitmiseks, siis erasektori vastajad töid eesmärkidena välja lepingute täitmise ja teenuste osutamise. Valdkondade esindajateks, kes puutuvad organisatsioonides kokku isikuandmete töötlemisega, on uuringu tulemustest lähtuvalt avalikus sektoris: kantselei, personal, sotsiaal-, haridus- ja noorsootöö valdkond, raamatupidamine, juristid, audiitorid, analüütikud, meditsiin, sisekontroll, ehitus-, kultuurivaldkond. Erasektoris on lisaks infotöötajatele personali valdkond, müügiosakond, turundus, juristid ja raamatupidamine. Ühise nimetajana saab uuringu tulemustes esile tõsta mõlema sektori puhul juhtkonna nimetamise ning samuti leiti, et suuremal või vähemal määral puutuvad isikuandmete töötlemisega asutustes kokku kõik töötajad.

E3: Muidugi puutuvad kokku ainult isikud, kes omavad õigust ja nende tööülesanded on seotud isikuandmete töötlemisega ja seda ka ainult vajalikus ulatuses. Aga tegelikult saab öelda, et suuremal või vähemal määral töötlevad kõik meie töötajad isikuandmeid.

Privaatsust puudutavad probleemid erinesid avaliku ja erasektori osas oluliselt. Avaliku sektori puhul toodi kitsaskohana välja asjaolu, et ühelt poolt kohustab seadus teavet avalikustama, teisalt tuleb kaitsta isikuandmeid. Seega nii infotöötajate, kui teiste töötajate eksimuse tulemusena võidakse avalikustada privaatset informatsiooni dokumendiregistris või asutuse kodulehel. Vigade tekkimise põhjusteks peeti nii lohakust kui regulatsioonide mittetundmist, mistõttu töötajad ei kehtesta dokumentidele juurdepääsupiirangut ning saab võimalikuks andmete vaikimisi avalikustamine.

A4: Tihti on see kinni isiku enda mugavuses ning eeldusel, et teised teevad töö ära – peetakse liiga tehniliseks tööks, mida sisuainimene tegema ei peaks. On isikuid, keda saab koolitada, millega nende teadmine täieneb, probleem laheneb, kuid on inimesi, kes seda kohustust siiski ei tee, vaid peavad infotöötaja ülesandeks.

Probleeme valmistavad olukorrad, kus kolmandad isikud soovivad infotöötajalt juurdepääsupiiranguga teavet, sealhulgas teiste inimeste isikuandmeid, saamata aru, et selline töötlemine ilma seadusliku aluseta on tõsine rikkumine. Lähtudes uuringu tulemustest saab väita, et praktikas on tavapärased juhused, kus avaliku sektori infotöötaja poole pööratakse ja soovitakse teiste isikute andmete avaldamist. Samas esineb ka vastupidine situatsioon, kus isik pöörub asutuse poole sooviga saada põhjendusi, miks tema andmeid on töödeldud (vaadatud registrist).

A3: Tooksin näitena selle, et kodanikud ei saa aru, mis on privaatsed isikuandmed. Ka töökaaslased. Minul on juurdepääs programmile pereregister, kus päringuid tehes on võimalik saada kõik andmed isikute kohta. Sageli pööratakse minu poole, et kuule vaata, kuna sellel isikul sünnipäev on ja kui vanaks ta saab või vaadake kuhu sissekirjutus on. Ja siis saan pahameele osaliseks kui selgitan – nii see ei käi. Minu päringuid kontrollib Siseministeerium ja ei aktsepteeri põhjendust, et tahtsin teada kuna kellegi sünnipäev on.

Probleemina tõstatati ka paberdokumentidel privaatsete andmete kaitse vajaduse suuremat teadvustamist ning selle tagamist, mis seisneb näiteks töötajate süstemaatilises kontrollimises paberkandjate hoidmise osas. Rikkumiste peamiste põhjustena nähti nii teenistujate vähest teadlikkust kui ükskõiksust.

Erasektori infotöötajate poolt antud vastuste analüüsimisel selgus, et probleemiks on kliendiandmete õigsuse ja täielikkuse kontrollimine. Ebakvaliteetsete, mittetäielike või valeandmete avaldamise põhjused tulenevad klientide hirmust riigi sunniaparaadi, maksuameti ees või ka soovist probleemi enda kasuks kirjeldada. Võimaliku kitsaskohana toodi välja ka töötajate teadlikkuse puudumist, mis on privaatne informatsioon ja kuidas seda nõuetekohaselt töödeldakse ning selle tagajärjel tekkida võivat organisatsiooni maine- ja finantskahju. Kirjeldatud probleemi tekkepõhjuseks peeti vähest informeeritust 25.05.2018 kohaldatava regulatsiooniga kaasnevatest muudatustest. Lisaks pidasid klientidega kontaktsuhtluses olevad infotöötajad oluliseks vajadust olla tähelepanelik ja hoolas, et ühe kliendi andmed ei satuks kättesaadavaks teistele klientidele ja kõrvalistele isikutele.

E4: Suurim probleem on andmete õigsuse ja täielikkuse kontrollimine. Näiteks esineb klientidel raskusi oma telefoninumbrite ja muu õigesti kirja panemisega. Tihti esineb ka otsest valeandmete esitamist, mõnede kontaktandmete esitamata jätmist, probleemi kirjeldamisel valikuliselt dokumentide esitamist jne.

Isikuandmete töötlemisel ja kaitsel tekkivate probleemide korral otsivad vastajad abi seadustest, Andmekaitse Inspektsiooni juhistest. Avaliku sektori infotöötajad töid tavapärase praktikana välja küsimuste korral Andmekaitse Inspektsiooni poole pöördumise, andmekaitse reeglite vastu eksinud teenistujate teavitamise tuvastatud rikkumisest ning koolitamise ja samuti toimunud rikkumiste informatsiooni edastamise ülematele. Erasektori teenistujad nimetasid asutuse poolt välja töötatud privaatsuspoliitikast ja juhenditest abi otsimist. Samuti kontrollitakse kahtluse korral klientide andmeid erinevatest netiallikatest ning vesteldakse veenmaks neid asutuse poolt turvalises andmetöötluses.

E2: Juhindun oma asutuse konfidentsiaalse teabe kaitse juhendist. Teenuste juhendist ning eeskirjadest ja meie organisatsiooni kliendiandmete töötlemise põhimõtetest, seadusi vaatan ja Andmekaitse Inspektsiooni lehte ikka.

Uuringu tulemused näitasid, et isikuandmete töötlemisel tõstatuvate probleemide korral pöörduvad avaliku sektori infotöötajad oma organisatsioonis juristi (juriidilise osakonna), infoturbspetsialisti, vahetu ülema ja juhtkonna poole, ühtlustatakse infotöötajatega praktikaid, arutatakse printsiipe. Erasektori vastajad pöörduvad juhtkonna poole, asutuses, kus on tööl jurist, konsulteeritakse temaga.

Seega saab kokkuvõtteks öelda, et privaatsust defineerivad nii avaliku kui erasektori töötajad ühtemoodi. Kui avaliku sektori infotöötajad rõhutasid privaatsete andmete mõiste sisustamisel organisatsiooni teenistujate kontaktandmete, terviseandmete olulisust ja töölepingu tingimusi, siis erasektori infotöötajad tõid lisaks välja kliendiandmed. Erinevad on sektorites ka isikuandmete töötlemisega seonduvad probleemid. Kui avalikus sektoris on suurimaks ohuallikaks vaikumisi avalikustamine, siis erasektoris peetakse väljakutseteks kliendiandmete täielikkuse ja kaitsega seonduvat.

3.2. Isikuandmete kaitseks rakendatavad praktikad

Mõlemas sektoris rakendatakse meetmeid hoidmaks ära konfidentsiaalset teavet sisaldava informatsiooni õigusliku aluseta sattumine kolmandate isikute ja juurdepääsuõigust mitteomavate isikute valdusesse. Avaliku sektori infotöötajad tõid eraldi punktidenä välja järgmised abinõud:

- juurdepääsupiirangute seadmise kohustus kõikidel dokumendi registreerijatel ja koostajatel;
- logide pidamise kohustus;
- isikuandmeid sisaldavate dokumentide hoidmise kohustus lukustatud kappides;
- arvuti lukustamine alati, kui ollakse sellest eemal;
- arvuti ekraanikaitse kasutamine (nii koht- kui sülearvutitel);
- klientide identifitseerimiskohustus, välja arvatud juhul kui on tegemist üldise teabega, mis on avalik;
- asutusesiseste juhendite koostamine teenistujatele, kuidas isikuandmeid sisalduva infoga käituda;
- iga-aastased küberhügieeni testid teenistujatele;
- eksimuste tuvastamine ja eksinud teenistujate juhendamine;
- registritele juurdepääsu võimaldamine vastavalt tööalastele ülesannetele ja teadmishäädusele.

Erasektori puhul loetleti tegevusi nagu paberandmete hoidmine lukustatavas kontorimööblis, keeld mitte jätta andmeid järelvalveta, kohustus kasutada turvatud arvutivõrku. Interneti teel edastamisel kasutatakse anonümiseerimist, juurdepääs elektroonilisel kujul andmetele võimaldatakse rolli- ja vajadusepõhiselt, kontoriruumides kasutatakse valvesignalisatsiooni, kehtestatud on sisekorrareeglid ja välja on töötatud asutuse infosüsteemide kasutamise kord.

E1: Isikuandmeid kogutakse paber kandjal, neid säilitatakse lukustatavates kappides, ligipääs üksnes tööülesandeid täitval juristil või büroojuhil. Aruanded koostame arvutis, arvutivõrk on turvatud. Interneti teel edastame ainult anonüümitud infot. Kontor on turvatud.

Küsimusele, kuidas oleks võimalik organisatsioonis privaatsuse kaitset veelgi tõhustada, jagunesid vastused mõlemas sektoris kaheks: pooled vastajatest leidsid, et privaatsuse kaitse asutuses on juba piisavalt tagatud ja pooled pidasid vajalikuks tegeleda järjepidevalt töötajate koolitamisega, vältimaks inimfaktorist tingitud eksimusi. Erasektori infotöötaja tõi välja ka tööruumidega seotud võimaliku kliendi privaatsuse riive vähendamise ning arhiivi korrastamise vajaduse.

E1: Tagamaks telefonikonsultatsioonide privaatsust võiks veel üks eraldi ruum olla. Arhiivi peab korrastama ja säilitustähtjaid üle vaatama.

Isikuandmete kaitse valdkonna eest vastutaja määramisel erineb avaliku ja erasektori praktika oluliselt. Kui avaliku sektori osas näitasid tulemused, et enamus juhtudel oli valdkonna eest vastutav infotöötaja, siis erasektoris oli selleks juhatus, ühel juhul ka personalitöötaja. Infotöötaja rolli andmekaitse valdkonnas pidasid kõik vastajad oluliseks. Dokumendihaldur on paljudel juhtudel esimeseks kontaktisikuks ja informatsiooni töötlejaks, tema ülesandeks peetakse privaatsete andmete töötlemise turvalisuse ja õiguspärasuse tagamist. Avalikus sektoris on lisaks eeltoodule infotöötaja ülesandeks andmekaitsealaste koolituste ja teavituse korraldamine, valdkonnas vajalike asutusesiseste õigusaktide ja haldusaktide koostamine. Tõhusaks isikuandmete kaitseks pidas avalik sektor oluliseks kõikide organisatsiooni tegevusalade esindajate koostööd, samas kui erasektoris rõhutati infotöötajate, juhtkonna, personalitöötajate ning juristide kaasatust.

A2: Tõhus andmekaitse eeldab nii juhtkonna kui kõigi valdkonna esindajate koostööd. Kui keegi nendest andmekaitse nõuetest kinni ei pea, võib see kaasa tuua andmete vale kasutuse.

Töötajate teadlikkuse tõstmise osas joonistus välja järgnev: avaliku sektori asutustes tegeleti sisekoolitustega, sealhulgas infotunnid uutele töötajatele juurdepääsupiirangute määramise temaatika selgitamiseks ning infoturbe valdkonnas, regulaarsed infoturbe ja dokumendihalduse alased kordavad koolitused ning isikuandmete kaitse olulisuse teadvustamine. Erasektoris toodi välja nii sise- kui avatud koolitusi, mis koosnesid praktilisest õppest (konkreetses infosüsteemi kasutamine) ja teoreetilisest isikuandmete kaitset puudutavast osast, nagu põhimõtete

tutvustamine, turvaline meilivahetus. Mõlema sektori puhul oli üks neljast vastajast, kelle organisatsioon ei tegelenud andmekaitse valdkonnas töötajate koolitamise ja teadlikkuse tõstmisega.

A1: Kord kuus toimuvad infotunnid, kus pöörame tähelepanu, selgitame, tutvustame vastavaid kordasid. Väga palju tuleb rääkida, rääkida ja veelkord rääkida, et arvutite ja postkastide paroolid peavad olema tugevad, neid tuleb teatud aja tagant vahetada. Inimesed on mugavad ja muidugi nõuab see töötajalt pingutust, kui pidevalt on vaja siseneda uute paroolidega, neid meeles pidada.

Uuringu tulemuste analüüs näitab, et täiendavate lisateadmiste vajadus on eelkõige just andmekaitserreformiga seonduvate uuenduste osas. Küsimusi tekitab, mida uus määrus kaasa toob ja mis sellega seoses muutub. Detailsemalt toodi teemadena välja mõjuhinnangu koostamine, andmete ülekantavus, õigus olla unustatud. Avaliku sektori osas tõi vastaja välja infosüsteemide muutmisest tuleneva praktilise koolituse vajaduse.

A3: Samas pereregistris muudetakse pidevalt midagi, aga ministeeriumi koolitused ei jõua meie töötajateni. Peab ise hakkama saama.

Nii avaliku kui erasektori asutustes rakendatakse meetmeid vältimaks konfidentsiaalset teavet sisaldava informatsiooni õigusliku aluseta sattumist kolmandate isikute valdusesse. Tagamaks organisatsioonis tõhus andmekaitse on vajalik erinevate valdkondade esindajate ja juhtkonna koostöö. Kui avalikus sektoris vastutavad isikuandmete kaitse eest valdavalt infotöötajad, siis erasektoris on selleks juhtkond. Tulemused annavad alust väita, et personali teadlikkuse tõstmisele pööratakse tähelepanu suuremas osas asutustes. Täiendavalt vajaksid nii avaliku kui erasektori infotöötajad tutvustust EL isikuandmete kaitse üldmääruses (2016) ja selle rakendusaktides sätestatu osas.

3.3. Andmekaitserreformiga kaasnevad muudatused

2016. aastal kiitis Euroopa Parlament heaks isikuandmete kaitse üldmääruse (2016), millega asendati senine andmekaitse direktiiv. Tegemist on otsekohalduva määrusega, mis koos siseriiklike rakendusaktidega asendas Eestis isikuandmete kaitse seaduse (2016). Määruse kohaldamise aeg oli 25.05.2018. Intervjuud infotöötajatega viidi läbi perioodil 02.–07.04.2018, mis eelnes määruse kohaldamise tähtajale. Tulemuste peatüki kolmanda alateema moodustasid küsimused, mis

puudutavad andmekaitsereformi ja selle tulemusena toimuvaid muudatusi, nii infotöötaja ametiülesannetes kui organisatsioonis.

Vastajatel paluti välja tuua, kuidas mõjutab infotöötaja igapäevatööd EL isikuandmete kaitse üldmäärus (2016). Erasektoris jagunesid vastused kaheks, pooled vastanutest leidsid, et andmekaitsereform ei ole mõjutanud nende igapäevatööd ning samuti ei ole asutuses toimunud tegevusi, mis tulenevad regulatsioonide muutumisest. Teine pool vastajatest tõi välja, et asutus on alustanud protsesside ja protseduuride, mis on seotud isikuandmetega, ülevaatamist/kaardistamist; uute isikuandmete ankeetide ja kliendinõusolekute koostamist, mõjuhinna läbiviimist, arhiivi korrastamist ja säilitustähtaegade määramise ülevaatamist, asutusesiseste regulatsioonide väljatöötamist ja töötajate teadlikkuse tõstmist. Kõigi nende tegevuste juures on oluline roll infotöötajal, nii sisendi andjana, konkreetsete ülesannete täitjana, kui ka riskide maandamisel.

E1: Oleme pidanud üle vaatama kõik protseduurid, mis on seotud isikuandmete töötlemisega, koostama uue isikuandmete ankeedi, järgides andmete minimaalsuse põhimõtet ja sõnastanud ümber kliendi nõusoleku. Töös on veel arhiivi korrastamine, säilitustähtaegade määramine.

Avaliku sektori puhul jagunesid vastused samuti kaheks, kui üks osa uuringus osalejatest leidis, et muutusi igapäevatöös ei tule, kuna avalikus sektoris on antud nõuded kehtinud ka varem, siis teine pool infotöötajatest ei osanud küsimusele vastata, sest puudus täpsem informatsioon ja ettekujutus uuendustega kaasnevast. Sarnaselt jagunesid arvamused ka asutuses toimunud muudatuste osas. Pooltel juhtudel toodi välja andmekaitse spetsialisti positsiooni loomist, ülejäänutel puudus informatsioon organisatsioonis toimuvast. Avaliku sektori hinnangul on infotöötaja roll reformi rakendamisel eelkõige toetav, ta peab olema õigusaktidega ja regulatsioonidega kursis, kuid tuntakse, et üldmäärus ei mõjuta otseselt igapäevatööd, täidetavaid tööülesandeid ja rolli. Leitakse, et koolituste ja teavituse korraldamine ning vajalike asutusesiseste õigusaktide ja haldusaktide koostamine jääb jätkuvalt nende ülesandeks. Samas ollakse äraootaval seisukohal ning soovitakse saada täpsemaid suuniseid.

Uuringu tulemused tõi välja, et infotöötajad on üksikutel juhtudel kokku puutunud isikute nõuete või päringutega, kus soovitakse teada, miks asutus nende isikuandmeid töötleb või on töödelnud. Avaliku sektori puhul nimetati ühel juhul teabenõude vormis kirjalikku pöördumist, millele vastamisega tegeles sisekontroll ja erasektori puhul suulist pöördumist müügiosakonda. Leiti, et andmekoosseisuga tutvumise soov ei ole uuringu läbiviimise ajal samuti aktuaalne, kuid peeti tõenäoliseks huvi kasvu, mille toob kaasa teema päevakajalisus ja inimeste teadlikkuse tõus.

Erasektori infotöötajal tõstatas sellest tulenevalt mure, kas tema poolt tehtavad tegevused ja andmete töötlemine on ikka piisavalt korrektne.

A1: Tundub, et see on tihenev soov ning paljuskki tänu sellele, et inimesed teadvustavad endale aina rohkem andmete kogumist ja ka sellega kaasnevaid oht, kindlasti ka võimalusi.

Alateema lõpetuseks soovisin teavet, millised isikuandmete kaitse üldmäärusest (EL..., 2016) tulenevad regulatsioonid on infotöötajate arvates kõige raskemini rakendatavad ning mil määral tagavad olemasolevad infosüsteemid õiguste, nagu andmete kustutamine ja ülekantavus, realiseerimist. Valdavalt ei osatud kummalegi küsimusele vastata põhjendades seda informatsiooni puudumisega ning vähese kursisolekuga üldmääruses sätestatuga, mis ei võimalda arvamust avaldada. Avaliku sektori valim pigem eeldas infosüsteemidelt vastavate funktsionaalsuste olemasolu, mis toetavad isiku õiguste realiseerimist, kuid ei olnud selles kindel. Erasektoris tõid infotöötajad probleemina välja andmete ülekantavuse ning asutustes tegeleti uuringu läbiviimise ajal selle lahendamisega. Samuti viidati erasektori finantspõhisele lähenemisele ning võimalikule teadliku riski võtmisele, kui ei suudeta kõiki norme vajalikus mahus täita.

E3: Arvan, et sellele ei ole erasektoris väga palju tähelepanu pööratud. Tihti jääb see tahaplaanile just sellepärast, et asutus on, kas liiga väike või finantsiliste võimaluste taha. Hinnatakse riske – kui suur on tõenäosus, et probleem tekib ning kui palju läheb selle ärahoidmine maksma võrdluses tekkida võivate kahjudega – trahvid, maine ja muu.

Uuringu tulemused näitasid, et infotöötajate teadlikkus reformiga kaasnevast on pigem madal. Erasektoris on kaasatus organisatsiooni poolt läbiviidavatesse tegevustesse suurem. Samas leiti, et avalikus sektoris on nõuded kehtinud ka varem ning palju uuendusi andmekaitsereformiga ei kaasne.

Järgnevalt toon uuringu tulemuste paremaks visualiseerimiseks Tabelis 1 välja peamised avaliku ja erasektori sarnasused ning erinevused.

Tabel 1. Uuringu tulemuste peamised sarnasused ja erinevused

| TEEMA | AVALIK SEKTOR | ERASEKTOR |
|--------------------------------|---|-----------|
| Privaatsuse mõiste sisustamine | Isiklik ja eraeluline informatsioon, õigus ise otsustada selle avaldamise või varjamise üle | |

| | | |
|---|--|---|
| Privaatsed andmed | Sotsiaalvaldkonna andmed, teenistujate kontaktandmed, terviseandmed, töölepingu tingimused | Kliendiandmed |
| Infotöötaja töö seotus privaatsusega | Olulisel määral, töötleb isikuandmeid | |
| Isikuandmete töötlemise eesmärk | Seadus, põhimäärus | Teenuste osutamine, lepingute täitmine |
| Isikuandmete töötlemisega puutuvad kokku | Valdav enamus asutuse töötajatest, oluline juhtkonna toetus/kaasatus | |
| Probleemid | <ul style="list-style-type: none"> - Ekslik avalikustamine, - kolmandate isikute infonõuded, - teabenõuded töötlemise aluse kohta, - paberdokumentide kaitse | <ul style="list-style-type: none"> - kliendiandmete õigsuse ja täielikkuse kontrollimine, - personali vähene teadlikkus, - kliendiandmete kaitse |
| Abi otsitakse | Seadustest, Andmekaitse Inspeksioonist, juhtkonnalt | |
| Täiendavad tegevused probleemide korral | <ul style="list-style-type: none"> - Eksinud teenistuja koolitamine, - koostöö juristi, infoturbespetsialisti ja kolleegidega | <ul style="list-style-type: none"> - kliendiandmete kontroll, - kliendisuhtlus, - asutuse privaatsuspoliitikast juhendumine, - koostöö juristidega. |
| Rakendatavad meetmed | Rakendatakse nii füüsilisi, infotehnoloogilisi, kui organisatsioonilisi meetmeid, sealhulgas rollipõhist juurdepääsu infosüsteemidele, paberdokumentide hoidmist lukustatavas kontorimööblis, sisekorrareeglite kehtestamist jne | |
| Spetsiifilised meetmed | Juurdepääsupiirangute seadmise kohustus, logide pidamine, identifitseerimiskohustus, info- ja kommunikatsioonitehnoloogia alased testid, seire eksimuste tuvastamiseks | Anonümiseerimine andmete edastamisel |
| Privaatsuse kaitse tõhustamine | ½ vastajatest leidsid, et privaatsuse kaitse on piisavalt tagatud, ½ pidas vajalikuks personali täiendavat koolitamist | |
| Isikuandmete kaitse valdkonna eest vastutaja asutuses | Infotöötaja | Juhtkond |

| | | |
|---|--|---|
| Infotöötaja roll andmekaitse valdkonnas | Lisaks andmete töötlemisele koolituste ja teavituse korraldaja | Esmane kontaktisik ja andmete töötleja |
| Täiendav koolitusvajadus | Eelkõige andmekaitsereformiga kaasnevate uuenduste osas | |
| Reformi mõjud igapäevatööl | 50% vastajatest leidis, et mõju puudub | |
| Infotöötaja roll reformi rakendamisel | Eelkõige toetav, sealhulgas koolitaja roll | Infotöötaja kaasatud asutuses protsesside kaardistamise, regulatsioonide ja dokumentatsiooni väljatöötamise ning riskide maandamisega seotud tegevustesse |
| Päringud isikuandmete koosseisu, töötlemise kohta | Pigem erandlikud | |
| Infosüsteemide funktsionaalsus | Pigem eeldatakse, et tagab andmesubjekti õigusi | Probleemiks andmete ülekantavuse tagamine. Regulatsioonide täitmisele eelneb finantspõhine riskide hindamine |

Toetudes uuringu tulemuste analüüsile saab väita, et mõlema sektori infotöötaja töö on otseselt seotud privaatsusega, seda eeskätt läbi andmetöötluse. Kui avalik sektor rõhutab pigem personali andmete kaitset, siis erasektor käsitleb teemat kliendikesksena. Suurimad erinevused infotöötaja vaatenurgast tulenevad just tema rollist, samuti valdkonna eest vastutuse määramisel ja igapäevatöös tõstatuvate probleemide osas. Oluliseks sarnasuseks on see, et sõltumata sektorist tuntakse vajadust EL isikuandmete kaitse üldmäärust (2016) ja selle rakendusakte käsitlevate koolituste järele.

4. DISKUSSION JA JÄRELDUSED

Lõputöö eesmärgiks oli välja selgitada privaatsust puudutavad praktilised väljakutsed avaliku ja erasektori infotöötaja töös. Käesolevas peatükis esitan järeldused, milleni olen jõudnud tulemusi analüüsides ning arutlen nende üle laiemas kontekstis.

Infotöötaja puutub oma igapäevatöös kokku konfidentsiaalse informatsiooni ja isikuandmetega (Dokumendihalduri kutsestandard, 2014), mille töötlemine on väga tihedalt seotud õigusega privaatsusele. Sagedasemad probleemid avaliku sektori dokumendihalduri jaoks on isikuandmete ekslik avalikustamine, surve avaldada juurdepääsupiiranguga teavet ja paberkandjal andmete kaitse; erasektori infotöötaja hinnangul on kitsaskohaks kliendiandmete kvaliteet, nende kaitse ning rikkumistega kaasnev võimalik asutuse maine- ja finantskahju. Töötleja kohustus järgida andmete kvaliteedi põhimõtet tuleneb EL isikuandmete kaitse üldmäärusest (2016) ning kajastus ka enne reformi kehtinud isikuandmete kaitse seaduses (2016). Lisaks kliendiandmete kaitsele on oluline tagada kõikide isikuandmete, sealhulgas ka personali andmete õiguspärane töötlemine.

Isikuandmete kaitseks rakendatavad praktikad on sümbioos erinevate distsipliinide kokkupuutest ning kasutusel on vastavalt õigusaktides sätestatule nii füüsilised, infotehnoloogilised, organisatsioonilised meetmed kui reeglid nende elluviimiseks (EL..., 2016; Handbook..., 2014: 94; isikuandmete kaitse seadus, 2016). Uuringu tulemused näitasid, et mõlemas sektoris on teadvustatud riske ja rakendatakse abinõusid nende maandamiseks, kuid käesolev lõputöö ei võimalda anda hinnangut meetmete piisavusele. Pigem annab see aluse väita, et pööratakse tähelepanu nii tehnilisele kui korralduslikule küljele ning teadvustatakse kaitse vajadust.

Intervjueeritavad leidsid, et suuremal või vähemal määral puutub isikuandmete töötlemisega asutustest kokku kogu personal, mis omakorda kohustab arvestama inimfaktorist tingitud potentsiaalse riskiga ning tegelema töötajate regulaarse koolitamise, teavitamisega andmeturbe valdkonnast, konkreetset ülesannete ja pädevuse jaotusega (Handbook..., 2014: 94). Analoogselt seminaritöö (Liister, 2018) ja Cooper'i (2016) uuringu tulemustele, peeti tõhusaks võimaluseks tõsta privaatsuse kaitset just läbi koolitamise. Asutuses kehtestatud protseduuride ebapiisav tutvustamine ning personali vähene koolitamine mõjutab õigusaktidest tulenevate privaatsust ja

isikuandmete kaitset puudutavate kohustuste täitmist. Samas leidis mõlemas sektoris asutusi, kus teavitamisele tähelepanu ei pööratud ning sellega rikuti üldmääruses (EL..., 2016) sätestatud vastutava töötaja kohustust.

Avalikus sektoris on privaatsuse ja isikuandmete kaitse valdkonnas koolitaja roll sageli infotöötajal ning selle jätkuvat täitmist peeti tõenäoliseks ka üldmääruse kohaldamise järel, hoolimata reformi tulemusena andmekaitse spetsialisti ametikoha, kelle ülesandeks on isikuandmete töötlemises osaleva personali koolitamine (EL..., 2016), loomisest.

Intervjuudes ei tõusnud otsesõnu esile infotöötaja ja infotehnoloogia või infoturbe spetsialistide vaheline koostöö, mida rõhutab kutsestandard (Dokumendihalduri..., 2014), kuid asutustes kasutusel olevate meetmete kirjeldused näitasid selle olemasolu, sest andmeturve on privaatsuse tagamisel võtmetähtsusega. Küll aga joonistus välja koostöö olulisus juhtkonnaga, kui uuenduste eestvedajaga, erasektori puhul ka valdkonna eest vastutajaga. Mõnevõrra üllatuslikult ei kajastanud uuringu tulemused vastutuse teemat pilvandmetöötajates või üldisemalt volitatud töötajatega seotud riske. Arvestades, et töötajate vastutuse reguleerimine on just üks EL isikuandmete kaitse üldmääruse (2016) eesmärkidest.

Infotöötajate teadlikkus 25.05.2018 kohaldunud andmekaitse reformist (EL..., 2016), organisatsiooni tegevustest selleks valmistumisel ja infotöötaja uuest rollist oli mõlema sektori infotöötajatel pigem madal. Erasektori infotöötajad olid kaasatud asutuses läbiviidavate protsesside ning infovarade kaardistamise juurde, samas kui avaliku sektori intervjuueeritavad leidsid, et reform ei too kaasa juba rakendatud ning isikuandmete kaitse seaduses (2016) sätestatud üldpõhimõtete muutumist, mistõttu suuri uuendusi sellega igapäevatoos ei kaasne. Määrus (EL..., 2016) sisaldab küll era- ja avaliku sektori jaoks olulisi erinevusi, kuid need seisnevad üksnes andmekaitse spetsialisti määramises ja tervikhindamise läbiviimise vajalikkuses, mitte aga põhimõistetes ja töötlemise reeglites.

Ühelt poolt on madal kaasatus, teisalt initsiatiivi mittehaaramine üllatav, arvestades nii dokumendihalduri kutsestandardis (2014), seminaritöös (Liister, 2018) ja käesolevas uuringus selgunud infotöötajate tööülesandeid ja rolli valdkonnas. Võimalus otsustusprotsessides kaasa rääkida aitaks ennetada hilisemaid probleeme reformi rakendamisel, tagaks selguse ülesannete ja vastutuse jaotumisel ning tõstaks seeläbi privaatsuse kaitset. Teenistujad on oma töös pühendunud, kui nad tunnevad, et nende arvamusega arvestatakse (Cornelissen, 2008).

Tulemused näitasid, et iseenda andmete kohta esitatud päringud, kus soovitakse informatsiooni andmekoosseisu ja töötlemise kohta, ei ole levinud, kuid infotöötajad eeldavad nende sagenemist. Nimetatud õiguse olemasolu suurendab andmesubjekti jaoks nii töötlemise läbipaistvust kui kontrolli oma isikuandmete üle (Euroopa Komisjon, 2010). Valdavalt ei teadnud infotöötajad, mil määral tagavad olemasolevad infosüsteemid andmete kustutamise ja ülekantavuse realiseerimist, kuid avalik sektor pigem eeldas vastavate funktsionaalsuste olemasolu. Erasektori infotöötajad pidasid probleemiks andmete ülekantavuse tagamist, mis on ka põhjendatud, kuna tegemist on uue mõistega. Samas kui õigus nõuda oma andmete kustutamist oli sätestatud juba isikuandmete kaitse seaduses (2016). Oluliseks aspektiks on ka see, et kustutamist saab nõuda üksnes andmete osas, mida töödeldakse nõusoleku alusel või mida töödeldakse õigusliku aluseta. Seaduse alusel töödeldavate ja säilitatavate andmete kustutamist andmesubjekt nõuda ei saa.

Leian, et isikliku informatsiooni uurimine on tähtis ja aktuaalne. Isikuandmed on kujunenud omaette käibeobjektiks ja omandanud rahaliselt mõõdetava väärtuse (Tikk, 2004), mistõttu tõuseb ka nende õiguspärase töötlemise olulisus. Lõputöös käsitletud teemat on võimalik edasi arendada mitmel viisil: üheks võimaluseks on uurida organisatsioonides, kus on asunud tööle andmekaitse spetsialist, toimunud ülesannete- ja pädevuse jaotumist andmekaitse valdkonnas just infotöötaja võtmes; teisalt uurida andmetöötajate kompetentsi ja kaardistada andmetöötluslane koolitusvajadus. Teema edasine uurimine aitab tuvastada võimalikke probleeme, parandada andmekaitse alast koostööd valdkondade vahel ning juhib organisatsioonide tähelepanu kitsaskohtadele, vähendades seeläbi ohtu andmesubjektide põhiõiguste riivele. Mida enam vastab privaatsuse objektiivne tagatus inimese subjektiivsetele ootustele, seda suuremaks võib hinnata ühiskonna stabiilsust ja paindlikkust privaatõiguse tagamisel (Tikk, 2004).

Käesoleva lõputöö eesmärgi saavutamiseks valitud kvalitatiivne uurimismeetod (semistruktureeritud intervjuu) sobis, sest intervjuudest selgus laiaulatuslik vaade privaatsust puudutavate väljakutsete kaardistamiseks. Üheks aspektiks, mida meetodi kriitika osas esile tõsta on uuritava teema delikaatsus ja sellest tulenev intervjuueeritavate valmisolek käsitleda probleeme. Kvantitatiivne meetod ja ankeedi täitmine annab vastajale võib-olla suurema anonüümsuse ning tagab kitsaskohtade julgema avaldamise. Samas õigustas aga kvalitatiivse meetodi valik end just seetõttu, et semistruktureeritud intervjuu paindlikkus võimaldas varieerida nii käsitletavate teemade järjekorda, kui ka esitada vajadusel täiendavaid küsimusi, eesmärgiga koguda püstitatud uurimisküsimustele vastamiseks võimalikult palju relevantset informatsiooni.

KOKKUVÕTE

Lõputöö on kirjutatud teemal „Privaatsust puudutavad praktilised väljakutsed infotöötaja töös“. Uuritav valdkond on oluline ja huvitav, kuna privaatsuse tajumine on tehnoloogia arenguga muutunud ning aina keerulisemaks saab ühe privaatsuse alustala, isikliku informatsiooni kaitsmine. Teema valiku ajendiks oli seminaritöö raames läbiviidud uuring, mis tuvastas mitmeid probleemkohti avaliku sektori infotöötaja töös privaatsuse tagamisel. Lähtuvalt varasematest uuringutest ja teooria peatükis käsitletust sõnastasin lõputöö eesmärgi ning püstitasin uurimisküsimused.

Töö eesmärgiks oli uurida ning välja tuua privaatsust puudutavad praktilised väljakutsed avaliku ja erasektori infotöötaja ametitegevuses. Selle täitmiseks viisin läbi nelja avaliku ja nelja erasektori infotöötajaga semistruktureeritud intervjuud, millede tulemused näitasid, et dokumendihalduse eest vastutavate töötajate ametiülesanded on otseselt seotud privaatsuse tagamise ning isikuandmete kaitsega. Kui avalikus sektoris on probleemide raskuspunkt seotud teabe avalikustamise ja sellele juurdepääsu piiramisega, siis erasektori infotöötaja jaoks on väljakutseks eelkõige kliendiandmete tervikluse tagamine.

Lisaks asutustes isikuandmete kaitseks rakendatavatele füüsilistele, infotehnoloogilistele ja organisatsioonilistele meetmetele, tagamaks andmete terviklus, käideldavus ja konfidentsiaalsus, peavad infotöötajad väga oluliseks koostööd teiste valdkondade esindajatega, samuti teiste andmetöötajatega ning juhtkonna poolset toetust, sealhulgas praktikate juurutamisel ja muutuste rakendamisel. Andmetöötlusriskide maandamise seisukohalt peetakse prioriteediks asutuse personali järjepidevat koolitamist.

Dokumendihalduse eest vastutavate teenistujate teadlikkus ja kaasatus andmekaitse reformi rakendamisse oli pigem madal. Andmekaitse reformi mõju infotöötaja igapäevastele tööülesannetele oli vähene või puudus üldse. Üldmääruses (2016) sätestatud „õiguse olla unustatud“ ja andmete ülekantavuse realiseerimise osas käsitleti probleemina pigem andmete ülekantavuse tagamist, samas avaliku sektori infotöötajad siiski eeldasid infosüsteemidelt

vastavate funktsionaalsuste olemasolu. Arvestades dokumendihalduri rolli ja tööülesandeid, oleks asutustel otstarbekas suuremal määral rakendada infotöötajate teadmisaasi andmekaitse valdkonnas ning tuua neid läbiviidavate tegevuste nagu infovarade ja protsesside kaardistamine, dokumentide uuendamine, juurde.

Uuringu tulemustele toetudes saab väita, et infotöötajatel on privaatsuse kaitsel asutustest täita oluline roll ning seda ka reformi järgselt. Märksõnadena tõstaksid vajadus koolituste järele ning koostöö ja otsustusprotsesside juurde kaasamise olulisuse.

Käesolev lõputöö kaardistas privaatsust puudutavad praktilised väljakutsed infotöötaja töös nii avalikus kui erasektoris ning tõi välja soovitud asutustele edasisteks tegevusteks. Läbiviidud uuringu tulemused annavad ülevaate andmekaitseõigusega seonduvatest praktikatest, probleemidest ning EL isikuandmete kaitse üldmääruse kohaldamiseks ettevalmistumisest infotöötaja vaates.

SUMMARY

The current thesis is written on the subject „ Privacy related practical challenges of an information professional’s work “. The area concerned is important and interesting since the perception of privacy has changed with the development of technology and one of the pillars of privacy law, the protection of personal information, is becoming increasingly complex. The primary driver for the choice of this subject was a research conducted during a seminar which identified several trouble spots in safeguarding the privacy of the work of an information professional’s work. The object of the thesis and the raised research questions are based on earlier research and the information covered in the theory chapter.

The object of the current paper was to examine and highlight the privacy related practical challenges in the occupational activity of both the public as well as private sector’s information worker. Semi-structured interviews were conducted with four public and four private sector information professionals to fulfil this task, the results of which showed that the official functions of the employees responsible for document management were directly related to safeguarding privacy and protection of personal data. If the main emphasis of problems in the public sector was related to publishing information and limiting access, then the biggest challenge for the information worker of the private sector was ensuring the integrity of customer information.

Information workers considered cooperation with representatives of other areas as well as with other data controllers and the support from management very important in addition to the physical, computerised and organisational measures applied in the organisation to protect personal data, to ensure the integrity, availability and confidentiality of data, including implementing practices and applying changes. Continuous training of the organisation’s personnel was considered a priority from the aspect of mitigating data processing risks.

The awareness and involvement of the data processing staff in the implementation of the data protection reform was relatively low. The impact of the data protection reform to the information worker’s daily tasks was poor or non-existent. The chapter in the Regulation (EU..., 2016), which

stipulated “the right to be forgotten” and the realisation of data transferability, considered ensuring data transferability as the main problem, where at the same time the information workers of the public sector assumed that such a functionality already existed in the information systems. Considering the role and work tasks of a data coordinator, it would have been appropriate for organisations to apply the data workers knowledgebase in the data protection area and bring them to the activities carried out, such as mapping information assets and processes as well as document renewal.

The results of the study showed that information workers have a key role to play in ensuring the protection of privacy in an organisation even after the reform. The need for trainings and the importance of cooperation and involvement in decision making processes were raised as keywords.

The current thesis mapped the privacy related challenges of an information professional’s job, both in the public as well as in the private sector, and made recommendations to the organisations for further actions to take. The results of the conducted research gave an overview of the practices and problems related to the data protection law as well as the preparations to apply the EU Data Protection Regulation in the perspective of an information professional.

KASUTATUD KIRJANDUS

1. Altman, I. (1976). Privacy: A Conceptual Analysis. *Environment and Behavior* 8:1, 7-30. Kasutatud 15.10.2017 <http://courses.ischool.berkeley.edu/i205/s10/readings/week11/altman-privacy.pdf>
2. Avaliku teabe seadus (16.01.2016) *Riigi Teataja* I. Kasutatud 11.12.2017 <https://www.riigiteataja.ee/akt/106012016007>
3. Baek, Y. M., Bae, Y., Jeong, I., Kim, E., Rhee, J. W. (2014). Changing the default setting for information privacy protection: What and whose personal information can be better protected? *Social Science Journal*, 51, 4, 523-533.
4. Cooper, A. (2016). *Safeguarding what's personal: privacy and data protection perspectives of Library Association of Ireland members*. Doktoritöö. Dublin Business School, Information and Library Management. Kasutatud 08.11.2017 http://esource.dbs.ie/bitstream/handle/10788/3050/msc_cooper_a_2016.pdf?sequence=1
5. Cornelissen, J. (2011). *Corporate Communication. A Guide to Theoy and Practice*. SAGE Publications Inc.
6. *Dokumendihalduri kutsestandard, tase* 6. (2014). Kasutatud 09.11.2017 <https://www.kutsekoda.ee/et/kutseregister/kutsestandardid/10541427>
7. Eesti Vabariigi põhiseadus (15.05.2015). *Riigi Teataja* I. Kasutatud 15.10.2017 <https://www.riigiteataja.ee/akt/115052015002>
8. EL isikuandmete kaitse üldmäärus. (04.05.2016). *Euroopa Liidu Teataja*. Kasutatud 18.03.2018 <http://www.privacy-regulation.eu/et/index.htm>
9. *Euroopa andmekaitse reform*. (2017). Kasutatud 09.11.2017 <http://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform>

10. Euroopa Liidu põhiõiguste harta (2012/C 326/02). *Euroopa Liidu Teataja*. Kasutatud 15.10.2017 <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A12012P%2FTXT>
11. Euroopa Komisjon. (2010). *Komisjoni teatis Euroopa Parlamendile, Nõukogule, Majandus- ja Sotsiaalkomiteele ning Regiooni Komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus*. Kasutatud 09.11.2017 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf
12. Euroopa Komisjon. (2014). *European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Ordinary legislative procedure - first reading. P7_TA(2014) 0212. Strasbourg: 12.03.2014 Kasutatud 18.03.2018 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//EN>
13. Finn, R., Wright, D., Friedewald, M. (2013). *Seven types of privacy*. European Data Protection: Coming of Age, 1-26. Kasutatud 15.10.2017 https://www.researchgate.net/profile/Michael_Friedewald2/publication/258892458_Seven_Types_of_Privacy/links/0c9605295d271f1575000000/Seven-Types-of-Privacy.pdf
14. Fried, C. (1968). Privacy. *The Yale Law Journal*, Vol 77, No 3, 475-493.
15. Handbook on European data protection law. (2014). *European Union Agency for Fundamental Rights. Council of Europe. Publications Office of the European Union*. Luxembourg: p 47. Kasutatud 26.03.2018 file:///C:/Users/kasutaja/Downloads/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf
16. Hirsjärvi, S., Remes, P. ja Sajavaara, P. (2010). *Uuri ja kirjuta*. Tallinn: Medicina.
17. Ilus, T. (2002). Isikuandmete kaitse olemus ja arengusuunad. *Juridica*, 7, 442.
18. Inimõiguste ja põhivabaduste kaitse konventsioon. (2010, 14, 54). *Riigi Teataja II*. Kasutatud 15.10.2017 <https://www.riigiteataja.ee/akt/13320295>
19. Isikuandmete kaitse seadus (06.01.2016). *Riigi Teataja I*. Kasutatud 15.10.2017 <https://www.riigiteataja.ee/akt/106012016010>

20. *Kuidas valmistuda andmekaitse üldmääruseks?* (2017). Kasutatud 27.03.2018
http://www.aki.ee/et/soovitused_maaruseks_valmistumisel
21. Laherand, M-L. (2008). *Kvalitatiivne uurimisviis*. Tallinn: Infotrükk OÜ.
22. Liister, M. (2018). *Privaatsust puudutavad väljakutsed infotöötaja töös avaliku sektori näitel*. Seminaritöö. Tartu Ülikool, Sotsiaalteaduste valdkond, Ühiskonnateaduste instituut, Infokorralduse õppekava.
23. Lomas, E. (2010). Information governance: information security and access within a UK context. *Records Management Journal*, 20, 182-198.
24. MacDonald, D. A., Streatfeild, C. M. (2014). PERSONAL DATA PRIVACY AND THE WTO. *Houston Journal of International Law*, 36, 3, 625-653. Kasutatud 01.04.2018
<http://www.hjil.org/articles/hjil-36-3-macdonald-streatfeild.pdf>
25. Maruste, R. (2004). *Konstitutsionalism ning põhiõiguste ja –vabaduste kaitse*. Tallinn: Kirjastus Juura.
26. Männiko, M. (2011). *Õigus privaatsusele ja andmekaitsele*. Tallinn: Kirjastus Juura.
27. Myburgh, S. (2003). Education directions for new information professionals. *Australian Library Journal*, 52, 3, 213-227. Kasutatud 09.11.2017
<http://www.tandfonline.com/doi/pdf/10.1080/00049670.2003.10721549>
28. Nõmper, A., Tikk, E. (2007). *Informatsioon ja õigus*. Tallinn: Kirjastus Juura.
29. Palm, E. (2009). Privacy Expectation at Work – What is Reasonable and Why? *Ethic Theory Moral Practice* 2009/12, No 2.
30. *Pilvandmetöötlus*. (2014). Kasutatud 09.11.2017 <http://www.aki.ee/et/pilvandmetootlus>
31. Pilving, I. (2005). Õigus isikuandmete kaitsele. *Juridica* 2005/7. Kasutatud 15.10.2017
https://www.juridica.ee/juridica_et.php?document=et/articles/2005/8/93807.SUM.php
32. Shils, E. (1966). Privacy: Its Constitution and Vicissitudes. *Law and Contemporary Problems* 4/1/1, Vol. 31, Issue 2, 281-306. Kasutatud 15.10.2017
<https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3109&context=lcp>
33. Smith, J. H., Milberg, S. J., Burke, S. J. (1996). Information Privacy: Measuring Individuals Concerns About Organizational Practices. *MIS Quarterly*, 1996, Vol. 20, Issue 2, 167-196.
Kasutatud 08.11.2017

- http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/SmithMilbergBurke1996_MISQ_InfoPrivacy.pdf
34. Steinerova, J. (2001). *Human issues of library and information work*. Kasutatud 09.11.2017 <http://InformationR.net/ir/6-2/paper95.html>
 35. Sweeney, L. (2002). k-Anonymity: A Model for Protecting Privacy. *International Journal of Uncertainty, Fuzziness & Knowledge-Based Systems*, Vol. 10, Issue 5, 557-570. Kasutatud 15.10.2017 https://epic.org/privacy/reidentification/Sweeney_Article.pdf
 36. Tihanov, S. (2015). *Privaatsus ja isikliku informatsioon organisatsioonisisestes suhetes*. Magistritöö. Tartu Ülikool, majandusteaduskond. Kasutatud 08.11.2017 http://dspace.ut.ee/bitstream/handle/10062/47558/tihanov_stina.pdf
 37. Tikk, E. (2004). *Informatsioonilise enesemääratlemise rahvusvahelis-õiguslik raamistik, sisustamine Eesti õiguses ja selle praktika kohaldamisest veebikeskkonnas*. Magistritöö. Tartu Ülikool, õigusteaduskond. Kasutatud 09.11.2017 <http://dspace.ut.ee/bitstream/handle/10062/876/Tikk.pdf?sequence=5&isAllowed=y>
 38. *Vaikimisi ja lõimitud andmekaitse*. (2017). Kasutatud 26.03.2018 <http://www.aki.ee/et/andmekaitse-reform/vaikimisi-ja-loimitud-andmekaitse>
 39. Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G. J. (2008). INFORMATION ACCOUNTABILITY. *Communications of the ACM*, 51, 6, 82-87. Kasutatud 01.04.2018 <http://dig.csail.mit.edu/2008/06/info-accountability-cacm-weitzner.pdf>
 40. ÜRO inimõiguste ülddeklaratsioon (2013). *Välisministeeriumi kodulehekülg*. Kasutatud 15.10.2017 <http://vm.ee/et/uro-inimoiguste-ulddeklaratsioon>

LISAD

Lisa 1. Intervjuu kava

Tutvustus

Tere! Olen Tartu Ülikooli infokorralduse eriala III kursuse tudeng Monika Liister ja kirjutan lõputööd privaatsust puudutavatest väljakutsetest infotöötaja töös.

Küsimused

- 1) Milline on Teie/Sinu erialane haridus?
- 2) Palun kirjeldada, mida tähendab Teie/Sinu jaoks mõiste privaatsus.
- 3) Millised andmed on Teie/Sinu arvates privaatsed? Miks?
- 4) Kuidas on Teie/Sinu töö seotud privaatsusega?
- 5) Milliste valdkondade esindajad puutuvad Teie/Sinu asutuses kokku isikuandmete, sealhulgas delikaatsete isikuandmete töötlemisega?
- 6) Millistel eesmärkidel Teie/Sinu asutuses isikuandmeid töödeldakse?
- 7) Milliste tööülesannete raames puutute/puutud kokku isikuandmete töötlemisega?
- 8) Mis valmistab Teie/Sinu jaoks seoses isikuandmete töötlemisega kõige suuremaid probleeme? Palun too(ge) selle kohta näiteid.
- 9) Teie/Sinu hinnangul, millest need probleemid tulenevad?
- 10) Millistest allikatest probleemide tekkel abi otsite/otsid?

- 11) Kelle poole Te/Sa oma organisatsioonis pöördud, juhul kui peaks tekkima küsimus seoses privaatsete andmete töötlemisega või haldamisega?
- 12) Kirjelda(ge) palun meetmeid, mida Teie/Sinu organisatsioon rakendab isikuandmete kaitseks?
- 13) Kuidas võiks Teie/Sinu hinnangul privaatsuse kaitset organisatsioonis veel tõhustada?
- 14) Kelle vastutusalaks on Teie/Sinu asutuses isikuandmete kaitse valdkond?
- 15) Teie/Sinu hinnangul, milliste tegevusalade esindajate koostöö on asutuses tõhusaks andmekaitseks vajalik? Palun põhjenda(ge) oma arvamust.
- 16) Milliseks peate/pead infotöötaja rolli andmekaitse valdkonnas? Palun selgita(ge) täpsemalt oma arvamust.
- 17) Kuidas korraldatakse Teie/Sinu organisatsioonis töötajate teadlikkuse tõstmist isikuandmete kaitse teemal?
- 18) Mis valdkondade esindajad peaksid Teie/Sinu arvates Teie/Sinu organisatsiooni näitel olema andmekaitse regulatsioonidest kindlasti teadlikud?
- 19) Kas Teie/Sinu asutuse töötajaid on koolitatud seoses antud teemadega?
- 20) Kui on koolitatud, siis millele on koolitusel eelkõige tähelepanu pööratud?
- 21) Mille osas tunnete/tunned, et vajaksite/vajaksid veel koolitusi või lisateadmisi?
- 22) Kuidas on mõjutanud Teie/Sinu igapäevatööd 25.05.2018 kohalduv EL isikuandmete kaitse üldmäärus?
- 23) Milliseid muutuseid on asutus seoses reformiga ette võtnud?
- 24) Millised üldmäärusest tulenevad regulatsioonid on Teie/Sinu hinnangul kõige raskemini rakendatavad? Palun põhjenda(ge) oma arvamust.
- 25) Milline on infotöötaja roll organisatsioonis seoses reformiga läbiviidud ja läbiviidavates tegevustes?
- 26) Mil määral olete/oled oma töös kokku puutunud sellega, et isik soovib teada, miks asutus on tema isikuandmeid töödelnud?

27) Teie/Sinu hinnangul kui tavaline on, et isikud soovivad tutvuda organisatsiooni poolt nende kohta kogutud andmetega (andmekoosseisuga)?

28) Mil määral tagavad organisatsioonis kasutusel olevate infosüsteemide funktsionaalsused üldmääruses sätestatud isiku õigust andmete kustutamisele ja andmete ülekantavust?

Sooviksite/sooviksid veel midagi lisada?

Tänan, et leidsite/leidsid aega vastamiseks!

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, **Monika Liister**

(sünnikuupäev: 19.01.1978)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

Privaatsust puudutavad praktilised väljakutsed infotöötaja töös,
(*lõputöö pealkiri*)

mille juhendaja on **Maris Männiste, MA,**

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace'i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. Olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 25.05.2018